EXHIBIT C-1
EXEMPLARY PORTIONS OF PRIOR ART THAT TEACH OR SUGGEST EACH ELEMENT OF THE ASSERTED '661 CLAIMS
PATENT L.R. 3-3(C)

Claim 1 ('661 Patent)	**U.S. 5,944,833 to Ugon ("Ugon")**
A cryptographic processing device for securely performing a cryptographic processing operation including a sequence of instructions in a manner resistant to discovery of a secret by external monitoring, comprising:	Abstract – "The present invention relates to an improved integrated circuit for a microprocessor controlled by at least one program and the process for using the circuit which includes means which can decorrelate the running of at least one instruction sequence of a program from internal or external electrical signals of the integrated circuit." 1:44-60 – "This capability of being able to observe the running of a program in a microprocessor or a microcomputer is a major drawback when the microprocessor or microcomputer is used in high-security applications. In effect, an ill-intentioned individual would thus be able to know the successive states of the processor and use this information to gain knowledge of certain internal output data. It is possible to imagine, for example, that a given action on an external signal could take place at different instants as a function of the result of a determined security operation, such as the testing of confidential internal information or the decryption of a message, or even the integrity checking of certain information. Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used." 1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 2:2-7 – "One of the objects of the invention is to equip the circuit with means for preventing the type of investigation described above, and more generally for preventing observations, whether illicit or not, of the internal behavior of the circuit." 2:8-11 – "This object is achieved through the fact that the improved integrated circuit has means for decorrelating the running of at least one instruction sequence of a program from the internal or external signals of the circuit."

	2:12-13 – "According to another characteristic, the electrical signals of the circuit are timing, synchronization or status signals." 3:59-63 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers." Claim 1 – "A process including a main program having interrupt sequences arranged to execute at least one operation and at least one instruction sequence in a microprocessor in synchronization with internal or external electrical signals of an integrated circuit comprising means for decorrelating an execution of the at least one instruction sequence of the program from the internal or external electrical signals of the integrated circuit so that the execution of the at least one instruction sequence is desynchronized with respect to the internal or external electrical signals . . . ."
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	1:44-60 – "This capability of being able to observe the running of a program in a microprocessor or a microcomputer is a major drawback when the microprocessor or microcomputer is used in high-security applications. In effect, an ill-intentioned individual would thus be able to know the successive states of the processor and use this information to gain knowledge of certain internal output data. It is possible to imagine, for example, that a given action on an external signal could take place at different instants as a function of the result of a determined security operation, such as the testing of confidential internal information or the decryption of a message, or even the integrity checking of certain information. Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used." 1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 3:51-58 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash

	type, etc . . . or a combination of these memories." 3:59-4:3 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers. However, these microcomputers or microprocessors, which use a shift register with parallel input-outputs looped back to at least one of its inputs, wherein the shift is timed by an internal clock, to constitute the random number generator, use the external clock for sequencing the machine cycles of the microprocessor to execute the instruction to read the contents of the register." 4:40-44 – "In the invention, the random number generator (2) is used either to supply a random value to the various devices through the data bus (3) and load it into the various devices which will be described below, or to generate a pulse signal of variable periodicity at its output (22)." *See also* Figures 1, 2 (*e.g.*, element 3). Claim 7 – "The integrated circuit according to claim 4, characterized in that said integrated circuit includes logic circuits and connecting busses connected such that sequencing of operations of the microprocessor factors in times required to access logic circuits of the integrated circuit, including signal propagation times in the busses and through the logic circuits." *See also* U.S. Patent No. 5,068,894 (Issued Nov. 26, 1991) at, *e.g.*, 5:4-29.
(b) a source of unpredictable information;	2:8-11 – "This object is achieved through the fact that the improved integrated circuit has means for decorrelating the running of at least one instruction sequence of a program from the internal or external signals of the circuit." 2:14-34 – "According to another characteristic, the decorrelation means comprise one or more circuits generating a sequence of clock or timing pulses which are dispatched at random times. According to another characteristic, the decorrelation means comprise a random number generator which makes it possible to de-synchronize the execution of the program sequence in the processor . . . . According to another characteristic, the decorrelation means comprise a random interrupt generating system. According to another characteristic, the decorrelation means comprise the execution of secondary sequences in which the instructions and execution times are different and which are

	selected at random. According to another characteristic, the variable time of the secondary process depends on a value supplied by a random number generator." 3:59-61 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) . . . ." 4:40-48 – "In the invention, the random number generator (2) is used either to supply a random value to the various devices through the data bus (3) and load it into the various devices which will be described below, or to generate a pulse signal of variable periodicity at its output (22). In a microprocessor or microcomputer of the invention, the signals required for the loading and execution of the instructions can therefore be generated from randomly dispatched clock pulses . . . ." 9:55-10:20 – "For the random number generator (2), it is possible, for example, to use looped counters having different periods, which counters are initialized with a 'seed' (information) stored in a non-volatile memory (7). When the processor starts up, the counters factor in the stored value as the initial value. During the calculation, or at the end of the calculation, the non-volatile memory (7) is updated with a new value which will serve as a seed for initializing the counters at the next initialization. The interrupt generating circuit (4) can be designed so that the generation of interrupt pulses seen above can occur, for example, when the number generated has certain characteristics, such as equality with certain data of the program. This circuit (4) can also take on the value of one or more bits of one or more counters. It is also possible to produce a very good random number generator using a cryptographic algorithm (69), as shown in FIG. 5 or a hash function initialized by the 'seeds' (information) seen above. In this case, the generator can be in the form of a program which implements the algorithm executed by the processor (1) and which, for example, implements the cryptographic algorithm by receiving a variable stored in the non-volatile memory (7) and a key for generating an output stored in a buffer register (41). This output stored in the buffer register is then processed by a hardware or software decoding device (42) for generating either the decorrelated clock signal (IT) CLK2 or a signal for interrupting the processor (1). It is easy to see that this random number generator can also be used to generate the various random numbers seen above. Another way to produce a generator of this type is to amplify the voltage generated at the terminals of a so-called 'noise' diode and to shape the signals after a low pass filtering for preventing the noise pulses that are too rapid from disturbing the operation." Figures 1, 2, 4A, 7A, 7B.

	See also 2:48-50, 2:55-57, 2:63-65, 8:39-52.
(c) a processor:	3:51-58 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories." 3:59-61 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) . . . ." Figures 1, 2.
(i) connected to said input interface for receiving and cryptographically processing said quantity,	1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 3:51-58 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories." 3:59-63 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers."
(ii) configured to use said unpredictable information to conceal a correlation between externally monitorable signals and said secret during said processing of said	2:28-31 – "According to another characteristic, the decorrelation means comprise the execution of secondary sequences in which the instructions and execution times are different and which are selected at random." 5:46-67 – "Lastly, the device of the invention can also comprise a secondary program (6) which, as will be seen below, can generate a variable duration time which varies each time this secondary program (6) is called by the main program (5). Thus, the variant of embodiment represented in FIG. 1 allows the main program (5) to change the desired degrees of protection, either by triggering the sequencing of

quantity by modifying said sequence; and	the execution of one or more instructions with the aid of the decorrelated clock CLK2, or by deciding during the execution of an instruction sequence to introduce, or not to introduce, a randomly triggered interrupt handler, or by deciding during the execution of the sequence to introduce, or not to introduce, a jump to the secondary program (6), which also generates a process with a variable time, or even by combining these various possibilities. Thus, in a variant of the invention, this secondary program (6) can be constituted as represented in FIG. 8 by a plurality of sequences (61, 62, 63 . . . 6n) which are called at random; and each sequence (0, 1, 2 or 2^{n-1}) will implement a different set of instructions which will result in a variable processing time in each branch and different behaviors of the microprocessor." 8:31-36 – "It is also possible to produce a fifth simplified embodiment of the invention which does not use an interrupt. When the main program needs to be protected, it independently activates a secondary program, which generates a process of random length at instants it selects, either at the start or during execution, so as to scramble the various sequences." 9:38-54 – "It may also be seen that no matter what the variant of embodiment, the running of the main program occurs with an unpredictable sequencing which, depending on the variant, depends on the random number generator, on the random clock, on the secondary program, on the random interrupts, or on a combination of at least two of these devices. When the main program executes functions that are not sensitive from the point of view of security, it can also return to the external clock CLKE, for example in order to deliver output data to the external world or to mask the decorrelation interrupt in order to optimize the processing time. As soon as a security function is implemented, the main program (5) authorizes the random mode of operation by validating either the random clock or the decorrelation interrupt (or both) in order to 'scramble' the various operational signals, particularly by de-synchronizing the clock relative to the main program, or by calling the secondary program." Claim 1 – "A process including a main program having interrupt sequences arranged to execute at least one operation and at least one instruction sequence in a microprocessor in synchronization with internal or external electrical signals of an integrated circuit comprising means for decorrelating an execution of the at least one instruction sequence of the program from the internal or external electrical signals of the integrated circuit so that the execution of the at least one instruction sequence is desynchronized with respect to the internal or external electrical signals, characterized in that the process comprises at least one of the following steps: a) triggering the

	sequencing of one of at least one instruction or at least one operation with the aid of a random-pulse clock; b) randomly triggering the interrupt sequences; c) triggering the processing of a random sequence of instructions or operations during the execution of a main sequence of instructions or operations; d) combining at least two of steps a, b and c." Claim 8 – "The integrated circuit according to claim 4, characterized in that the decorrelation means comprises means for execution of a secondary program, the secondary program including a random choice of one of a plurality of sequences, the plurality of sequences including sequences each having a different set of instructions and a different execution time than all other ones of the plurality of sequences." Claim 9 – "The integrated circuit according to claim 8, characterized in that the secondary program sequence generates a variable duration, wherein the variable duration depends on a value supplied by a random number generator."
(d) an output interface for outputting said cryptographically processed quantity to a recipient thereof.	1:51-67 – "It is possible to imagine, for example, that a given action on an external signal could take place at different instants as a function of the result of a determined security operation, such as the testing of confidential internal information or the decryption of a message, or even the integrity checking of certain information. Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used. Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 3:51-4:3 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories. The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers. However, these microcomputers or microprocessors, which use a shift register with parallel input-outputs looped back to at least one of its inputs,

	wherein the shift is timed by an internal clock, to constitute the random number generator, use the external clock for sequencing the machine cycles of the microprocessor to execute the instruction to read the contents of the register." *See also* Figures 1, 2 (*e.g.*, element 3). Claim 7 – "The integrated circuit according to claim 4, characterized in that said integrated circuit includes logic circuits and connecting busses connected such that sequencing of operations of the microprocessor factors in times required to access logic circuits of the integrated circuit, including signal propagation times in the busses and through the logic circuits." *See also* U.S. Patent No. 5,068,894 (Issued Nov. 26, 1991) at, *e.g.*, 5:4-29.

Claim 2 ('661 Patent)	**U.S. 5,944,833 to Ugon**
The device of claim 1 wherein said input interface and said output interface are the same element.	1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 3:51-4:3 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories. The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers. However, these microcomputers or microprocessors, which use a shift register with parallel input-outputs looped back to at least one of its inputs, wherein the shift is timed by an internal clock, to constitute the random number generator, use the external clock for sequencing the machine cycles of the microprocessor to execute the instruction to read the contents of the register."

	See also Figures 1, 2 (*e.g.*, element 3). Claim 7 – "The integrated circuit according to claim 4, characterized in that said integrated circuit includes logic circuits and connecting busses connected such that sequencing of operations of the microprocessor factors in times required to access logic circuits of the integrated circuit, including signal propagation times in the busses and through the logic circuits."

Claim 4 ('661 Patent)	**U.S. 5,944,833 to Ugon**
The device of claim 1 wherein said cryptographic processing operation includes transforming a message with the Data Encryption Standard (DES).	2:1-7 – "One of the objects of the invention is...[to prevent] observations, whether illicit or not, of the internal behavior of the circuit." *See, e.g.*, "Data Encryption Standard," Federal Information Processing Standards Publication (FIPS PUB) 46-2, U.S. Department of Commerce, National Institute of Standards and Technology, Dec. 30, 1993 (suggesting, at 3, various implementations of DES; and describing, at 5, high level of protection provided by DES); Menezes, A.J. et al., HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC Press, Boca Raton at 223 and 250 (1997)(describing DES as a well known block cipher and a common element of cryptographic systems).

Claim 5 ('661 Patent)	**U.S. 5,944,833 to Ugon**
A cryptographic processing device for securely performing a cryptographic processing operation implementing a permutation in a manner resistant to discovery of a secret by external monitoring, comprising:	*See supra* disclosure regarding preamble of '661 patent claim 1. *See also* Menezes, A.J. et al., HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC Press, Boca Raton at 10 (1997)(describing permutations as functions often used in cryptographic constructs).
(a) an input interface for receiving a quantity to be cryptographically	*See supra* disclosure regarding '661 patent claim 1(a).

processed, said quantity being representative of at least a portion of a message;	
(b) a source of unpredictable information;	*See supra* disclosure regarding '661 patent claim 1(b).
(c) a processor:	*See supra* disclosure regarding '661 patent claim 1(c).
(i) connected to said input interface for receiving and cryptographically processing said quantity,	*See supra* disclosure regarding '661 patent claim 1(c)(i).
(ii) configured to use said unpredictable information to conceal a correlation between externally monitorable signals and said secret during said processing of said quantity by randomizing the order of said permutation; and	8:31-36 – "It is also possible to produce a fifth simplified embodiment of the invention which does not use an interrupt. When the main program needs to be protected, it independently activates a secondary program, which generates a process of random length at instants it selects, either at the start or during execution, so as to scramble the various sequences." (emphasis added) 9:38-54 – "It may also be seen that no matter what the variant of embodiment, the running of the main program occurs with an unpredictable sequencing which, depending on the variant, depends on the random number generator, on the random clock, on the secondary program, on the random interrupts, or on a combination of at least two of these devices. When the main program executes functions that are not sensitive from the point of view of security, it can also return to the external clock CLKE, for example in order to deliver output data to the external world or to mask the decorrelation interrupt in order to optimize the processing time. As soon as a security function is implemented, the main program (5) authorizes the random mode of operation by validating either the random clock or the decorrelation interrupt (or both) in order to 'scramble' the various operational signals, particularly by de-synchronizing the clock relative to the main program, or by calling the secondary program." (emphasis added)
(d) an output interface for outputting said cryptographically processed quantity to a recipient thereof.	*See supra* disclosure regarding '661 patent claim 1(d).

Claim 6 ('661 Patent)	U.S. 5,944,833 to Ugon
A cryptographic processing device implemented on a single microchip for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring, comprising:	Abstract – "The present invention relates to an improved integrated circuit for a microprocessor controlled by at least one program and the process for using the circuit which includes means which can decorrelate the running of at least one instruction sequence of a program from internal or external electrical signals of the integrated circuit." 1:44-60 – "This capability of being able to observe the running of a program in a microprocessor or a microcomputer is a major drawback when the microprocessor or microcomputer is used in high-security applications. In effect, an ill-intentioned individual would thus be able to know the successive states of the processor and use this information to gain knowledge of certain internal output data. It is possible to imagine, for example, that a given action on an external signal could take place at different instants as a function of the result of a determined security operation, such as the testing of confidential internal information or the decryption of a message, or even the integrity checking of certain information. Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used." 1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 2:2-7 – "One of the objects of the invention is to equip the circuit with means for preventing the type of investigation described above, and more generally for preventing observations, whether illicit or not, of the internal behavior of the circuit." 2:8-11 – "This object is achieved through the fact that the improved integrated circuit has means for decorrelating the running of at least one instruction sequence of a program from the internal or external signals of the circuit." 2:12-13 – "According to another characteristic, the electrical signals of the circuit are timing, synchronization or status signals." 3:59-63 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned

	above, are particularly known through the ST16XY family of microcomputers." Claim 1 – "A process including a main program having interrupt sequences arranged to execute at least one operation and at least one instruction sequence in a microprocessor in synchronization with internal or external electrical signals of an integrated circuit comprising means for decorrelating an execution of the at least one instruction sequence of the program from the internal or external electrical signals of the integrated circuit so that the execution of the at least one instruction sequence is desynchronized with respect to the internal or external electrical signals . . . ." *See also* 3:51-58 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories." (emphasis added)
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	1:44-60 – "This capability of being able to observe the running of a program in a microprocessor or a microcomputer is a major drawback when the microprocessor or microcomputer is used in high-security applications. In effect, an ill-intentioned individual would thus be able to know the successive states of the processor and use this information to gain knowledge of certain internal output data. It is possible to imagine, for example, that a given action on an external signal could take place at different instants as a function of the result of a determined security operation, such as the testing of confidential internal information or the decryption of a message, or even the integrity checking of certain information. Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used." 1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 3:51-58 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated

	with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories." 3:59-4:3 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers. However, these microcomputers or microprocessors, which use a shift register with parallel input-outputs looped back to at least one of its inputs, wherein the shift is timed by an internal clock, to constitute the random number generator, use the external clock for sequencing the machine cycles of the microprocessor to execute the instruction to read the contents of the register." 4:40-44 – "In the invention, the random number generator (2) is used either to supply a random value to the various devices through the data bus (3) and load it into the various devices which will be described below, or to generate a pulse signal of variable periodicity at its output (22)." *See also* Figures 1, 2 (*e.g.*, element 3). Claim 7 – "The integrated circuit according to claim 4, characterized in that said integrated circuit includes logic circuits and connecting busses connected such that sequencing of operations of the microprocessor factors in times required to access logic circuits of the integrated circuit, including signal propagation times in the busses and through the logic circuits." *See also* U.S. Patent No. 5,068,894 (Issued Nov. 26, 1991) at, *e.g.*, 5:4-29.
(b) a source of unpredictable information;	2:8-11 – "This object is achieved through the fact that the improved integrated circuit has means for decorrelating the running of at least one instruction sequence of a program from the internal or external signals of the circuit." 2:14-34 – "According to another characteristic, the decorrelation means comprise one or more circuits generating a sequence of clock or timing pulses which are dispatched at random times. According to another characteristic, the decorrelation means comprise a random number generator which makes it possible to de-synchronize the execution of the program sequence in the processor . . . . According to another characteristic, the decorrelation means comprise a random interrupt generating system. According to another characteristic, the

	decorrelation means comprise the execution of secondary sequences in which the instructions and execution times are different and which are selected at random. According to another characteristic, the variable time of the secondary process depends on a value supplied by a random number generator." 3:59-61 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) . . . ." 4:40-48 – "In the invention, the random number generator (2) is used either to supply a random value to the various devices through the data bus (3) and load it into the various devices which will be described below, or to generate a pulse signal of variable periodicity at its output (22). In a microprocessor or microcomputer of the invention, the signals required for the loading and execution of the instructions can therefore be generated from randomly dispatched clock pulses . . . ." 9:55-10:20 – "For the random number generator (2), it is possible, for example, to use looped counters having different periods, which counters are initialized with a 'seed' (information) stored in a non-volatile memory (7). When the processor starts up, the counters factor in the stored value as the initial value. During the calculation, or at the end of the calculation, the non-volatile memory (7) is updated with a new value which will serve as a seed for initializing the counters at the next initialization. The interrupt generating circuit (4) can be designed so that the generation of interrupt pulses seen above can occur, for example, when the number generated has certain characteristics, such as equality with certain data of the program. This circuit (4) can also take on the value of one or more bits of one or more counters. It is also possible to produce a very good random number generator using a cryptographic algorithm (69), as shown in FIG. 5 or a hash function initialized by the 'seeds' (information) seen above. In this case, the generator can be in the form of a program which implements the algorithm executed by the processor (1) and which, for example, implements the cryptographic algorithm by receiving a variable stored in the non-volatile memory (7) and a key for generating an output stored in a buffer register (41). This output stored in the buffer register is then processed by a hardware or software decoding device (42) for generating either the decorrelated clock signal (IT) CLK2 or a signal for interrupting the processor (1). It is easy to see that this random number generator can also be used to generate the various random numbers seen above. Another way to produce a generator of this type is to amplify the voltage generated at the terminals of a so-called 'noise' diode and to shape the signals after a low pass filtering for preventing the noise pulses that are too rapid from disturbing the operation."

	Figures 1, 2, 4A, 7A, 7B. *See also* 2:48-50, 2:55-57, 2:63-65, 8:39-52.
(c) a processor:	3:51-58 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories." 3:59-61 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) . . . ." Figures 1, 2.
(i) connected to said input interface for receiving and cryptographically processing said quantity,	1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 3:51-58 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories." 3:59-4:3 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers. However, these microcomputers or microprocessors, which use a shift register with parallel input-outputs looped back to at least one of its inputs, wherein the shift is timed by an internal clock, to constitute the random number generator, use the external clock for sequencing the machine cycles of the microprocessor to execute the instruction to read the contents of the register."
(ii) configured to use said unpredictable information to	2:28-31 – "According to another characteristic, the decorrelation means comprise the execution of secondary sequences in which the instructions and execution times are different and which are selected at

conceal a correlation between said microchip's power consumption and said processing of said quantity by expending additional electricity in said microchip during said processing; and	random." 5:46-67 – "Lastly, the device of the invention can also comprise a secondary program (6) which, as will be seen below, can generate a variable duration time which varies each time this secondary program (6) is called by the main program (5). Thus, the variant of embodiment represented in FIG. 1 allows the main program (5) to change the desired degrees of protection, either by triggering the sequencing of the execution of one or more instructions with the aid of the decorrelated clock CLK2, or by deciding during the execution of an instruction sequence to introduce, or not to introduce, a randomly triggered interrupt handler, or by deciding during the execution of the sequence to introduce, or not to introduce, a jump to the secondary program (6), which also generates a process with a variable time, or even by combining these various possibilities. Thus, in a variant of the invention, this secondary program (6) can be constituted as represented in FIG. 8 by a plurality of sequences (61, 62, 63 . . . 6n) which are called at random; and each sequence (0, 1, 2 or 2^{n-1}) will implement a different set of instructions which will result in a variable processing time in each branch and different behaviors of the microprocessor." *See also* 6:66-7:10 – "Another embodiment of a secondary program of variable duration can be comprised of defining an area of the program storage corresponding to the secondary program (6) in which a set of instructions is stored. Preferably, the instructions chosen require different numbers of machine cycles in order to be executed, as is known to be the case, for example, with the instructions J, CALL, RET, RST, PCHL, INX in relation to instructions requiring a number of shorter machine cycles such as ADC, SUB, ANA, MOV, etc. Thus, in this storage area, there are a certain number of available instructions having execution durations that are different from one another in terms of the number of machine cycles." (emphasis added) *See also* 5:67-6:43. 8:31-36 – "It is also possible to produce a fifth simplified embodiment of the invention which does not use an interrupt. When the main program needs to be protected, it independently activates a secondary program, which generates a process of random length at instants it selects, either at the start or during execution, so as to scramble the various sequences." 9:38-54 – "It may also be seen that no matter what the variant of embodiment, the running of the main program occurs with an unpredictable sequencing which, depending on the variant, depends on the random number generator, on the random clock, on the secondary program, on the random interrupts, or on a combination of at least two

	of these devices. When the main program executes functions that are not sensitive from the point of view of security, it can also return to the external clock CLKE, for example in order to deliver output data to the external world or to mask the decorrelation interrupt in order to optimize the processing time. As soon as a security function is implemented, the main program (5) authorizes the random mode of operation by validating either the random clock or the decorrelation interrupt (or both) in order to 'scramble' the various operational signals, particularly by de-synchronizing the clock relative to the main program, or by calling the secondary program." Claim 1 – "A process including a main program having interrupt sequences arranged to execute at least one operation and at least one instruction sequence in a microprocessor in synchronization with internal or external electrical signals of an integrated circuit comprising means for decorrelating an execution of the at least one instruction sequence of the program from the internal or external electrical signals of the integrated circuit so that the execution of the at least one instruction sequence is desynchronized with respect to the internal or external electrical signals, characterized in that the process comprises at least one of the following steps: a) triggering the sequencing of one of at least one instruction or at least one operation with the aid of a random-pulse clock; b) randomly triggering the interrupt sequences; c) triggering the processing of a random sequence of instructions or operations during the execution of a main sequence of instructions or operations; d) combining at least two of steps a, b and c." Claim 8 – "The integrated circuit according to claim 4, characterized in that the decorrelation means comprises means for execution of a secondary program, the secondary program including a random choice of one of a plurality of sequences, the plurality of sequences including sequences each having a different set of instructions and a different execution time than all other ones of the plurality of sequences." Claim 9 – "The integrated circuit according to claim 8, characterized in that the secondary program sequence generates a variable duration, wherein the variable duration depends on a value supplied by a random number generator."
(d) an output interface for outputting said cryptographically processed quantity to a recipient thereof.	1:51-67 – "It is possible to imagine, for example, that a given action on an external signal could take place at different instants as a function of the result of a determined security operation, such as the testing of confidential internal information or the decryption of a message, or even the integrity checking of certain information. Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used.

	Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 3:51-4:3 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories. The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers. However, these microcomputers or microprocessors, which use a shift register with parallel input-outputs looped back to at least one of its inputs, wherein the shift is timed by an internal clock, to constitute the random number generator, use the external clock for sequencing the machine cycles of the microprocessor to execute the instruction to read the contents of the register." *See also* Figures 1, 2 (*e.g.*, element 3). Claim 7 – "The integrated circuit according to claim 4, characterized in that said integrated circuit includes logic circuits and connecting busses connected such that sequencing of operations of the microprocessor factors in times required to access logic circuits of the integrated circuit, including signal propagation times in the busses and through the logic circuits." *See also* U.S. Patent No. 5,068,894 (Issued Nov. 26, 1991) at, *e.g.*, 5:4-29.

Claim 7 ('661 Patent)	**U.S. 5,944,833 to Ugon**
The device of claim 6 including program logic to activate said expending during said	5:46-6:43 – "Lastly, the device of the invention can also comprise a secondary program (6) which, as will be seen below, can generate a variable duration time which varies each time this secondary program (6) is called by the main program (5). Thus, the variant of embodiment represented in FIG. 1 allows the main program (5) to change the

processing.	desired degrees of protection, either by triggering the sequencing of the execution of one or more instructions with the aid of the decorrelated clock CLK2, or by deciding during the execution of an instruction sequence to introduce, or not to introduce, a randomly triggered interrupt handler, or by deciding during the execution of the sequence to introduce, or not to introduce, a jump to the secondary program (6), which also generates a process with a variable time, or even by combining these various possibilities. Thus, in a variant of the invention, this secondary program (6) can be constituted as represented in FIG. 8 by a plurality of sequences (61, 62, 63 . . . 6n) which are called at random; and each sequence (0, 1, 2 or 2^{n-1}) will implement a different set of instructions which will result in a variable processing time in each branch and different behaviors of the microprocessor. The sequences can be called at random; for example, after the main program has executed the jump to the secondary program, the latter loads, in the steps (64 and 65), a random value V originating from the memory (7) into two registers, for example R10 and R11, of the microprocessor (1). The secondary program increments this value V, then the program orders the storage of this incremented value (V+1) in the non-volatile memory NVM (7) in the step (66). This value stored in the non-volatile memory (7) is intended to be used later. The secondary program, in the step 67, then extracts n high-order or low-order bits in R10 in order to obtain a value r which will make it possible to indicate which program sequence among the secondary program sequences (61, 62, 63, . . . , 6n) is to be executed. Each secondary program sequence will produce a different process: for example, the sequence (0) is comprised, first of all, of the step 611 for transferring the content of the register R11 of the microprocessor into a register R12. In the step 612, the content of R12 is added to the carry value (CARRY), then in the step 613, an exclusive OR is executed between the content of the register R11 and the content of the register R12, and the result is placed in the register R12. In the step 614, the processor decrements R12; in the step 615, a test is carried out on the value of R12 to determine whether or not R12 is equal to zero. In the case where R12=0, the processor returns to the execution of the main program. In the opposite case, in the step 616, the secondary program (61) executes a rotation of the content of the register R10. The next step consists of extracting n bits of a determined order from the register R10, in order to then access one of the sequences determined by this value r in the secondary program. Thus, it is possible to access, for example, the sequence (2^{n-1}) which, in the step (6n1), is comprised of transferring the result of the multiplication of the values of R10 and R11 into R13 and R14. In the step (6n2), this sequence executes a rotation of R13 and R14, then, in the step (6n3), the content of R13 is transferred into R11. In the step (6n4), R11 is decremented in order to then, in the step (6n5), perform a test on the value R11. This test is comprised of determining whether or

	not the content of R11=3. If so, the process returns to the main program and if not, the program proceeds to the step (6n6) by rotating R10 to the left, then executing the instruction (67) in order to access a new secondary program sequence." 6:44-65 – "In the case where the secondary program is intended to be combined with a decorrelated clock or interrupt handlers, it is possible in a combination of this type to restrict oneself to one secondary program, thus producing a simpler process. A simplified secondary program of this type can be constituted by the following instructions: MOV B, R2 which is comprised of loading the register R2 into the microprocessor register B LOOP DCX B which is comprised of decrementing the register B with the value A JNZ B LOOP which is comprised of performing a test on the value of the register B and of looping back to the label LOOP if this value is different from zero. This sequence ends with an instruction to return to the instruction of the main program which immediately follows the last instruction executed before the jump to the secondary program (6). The register R2 is pre-loaded by an instruction of the main program (5), before the jump to the secondary program (6), with a random value supplied by the random number generator (2). Thus, the execution of the secondary program defined above will always generate a variable duration." 6:66-7:26 – "Another embodiment of a secondary program of variable duration can be comprised of defining an area of the program storage corresponding to the secondary program (6) in which a set of instructions is stored. Preferably, the instructions chosen require different numbers of machine cycles in order to be executed, as is known to be the case, for example, with the instructions J, CALL, RET, RST, PCHL, INX in relation to instructions requiring a number of shorter machine cycles such as ADC, SUB, ANA, MOV, etc. Thus, in this storage area, there are a certain number of available instructions having execution durations that are different from one another in terms of the number of machine cycles. The main program (5) comprises an instruction to jump to an indexed address whose index corresponds to the content of the register R2 and whose address corresponds to the first address of the area (6). The execution of this instruction of the main program (5) therefore causes the addressing by the processor (1), at random, of instructions whose execution durations will be different depending on the position addressed. In a known way, the random number generator (2) will be initialized at the start to a variable. This

	initial variable is contained in a non-volatile memory (7) and constituted, for example, by the last random value generated by the generator (2) before the pausing of the microprocessor (1). Thus, the microprocessor, controlled by a program it will execute, will be able to use this program to activate the means for decorrelating the instruction execution sequencing of this program by loading, for example, registers R2 or 8, or by calling secondary programs." 8:6-15 – "The organization of the programs executed by the processor can be carried out in such a way that the operation of the processor (1) is controlled by a genuinely protected operating system which chooses the type of scrambling to be used as a function of the type of program run by the machine. In this case, it is the operating system which manages, as it sees fit, the various signals resulting from the random number generator, the calibrator, the interrupts or commands from the phase shifting circuit, and the start up of the main and secondary programs." Figures 1, 5, 7A, 8.

Claim 8 ('661 Patent)	**U.S. 5,944,833 to Ugon**
The device of claim 7 including (a) program logic implementing said source of unpredictable information; and	5:20-45 – "The device can also comprise a register R2 which is loaded, either by the random number generator (2) with a random number, or by the main program (5) with a value determined by the program. This register R2 is totally or partially used by a logic circuit (4) for triggering an interrupt, which receives at one of its inputs the decorrelated clock signal CLK2 issuing from the output (95) of the calibration circuit (9). The output of the circuit (4) is sent through a gate (48) controlled by one or more bits of the register (8) to the interrupt input (12) of the CPU. The bit or bits of this register (8) play the role of an interrupt mask control, which is standard in certain microprocessors. When an interrupt is received at the interrupt input (12) of the processor, the interrupt handling program contained, for example, in the operating system or in the secondary program will introduce a different processing time for the interrupted sequence of the main program. It must be understood that there are two phases in the interrupt mode of operation. A first phase, in which the microprocessor controlled by the so-called main program authorizes the decorrelated operation by unmasking, for example, the interrupts. A second phase, in which the interrupt automatically reroutes the operation to the secondary program. This operation can actually occur without the intervention of the main program."

	5:46-6:43 – "Lastly, the device of the invention can also comprise a secondary program (6) which, as will be seen below, can generate a variable duration time which varies each time this secondary program (6) is called by the main program (5). Thus, the variant of embodiment represented in FIG. 1 allows the main program (5) to change the desired degrees of protection, either by triggering the sequencing of the execution of one or more instructions with the aid of the decorrelated clock CLK2, or by deciding during the execution of an instruction sequence to introduce, or not to introduce, a randomly triggered interrupt handler, or by deciding during the execution of the sequence to introduce, or not to introduce, a jump to the secondary program (6), which also generates a process with a variable time, or even by combining these various possibilities. Thus, in a variant of the invention, this secondary program (6) can be constituted as represented in FIG. 8 by a plurality of sequences (61, 62, 63 . . . 6n) which are called at random; and each sequence (0, 1, 2 or 2^{n-1}) will implement a different set of instructions which will result in a variable processing time in each branch and different behaviors of the microprocessor. The sequences can be called at random; for example, after the main program has executed the jump to the secondary program, the latter loads, in the steps (64 and 65), a random value V originating from the memory (7) into two registers, for example R10 and R11, of the microprocessor (1). The secondary program increments this value V, then the program orders the storage of this incremented value (V+1) in the non-volatile memory NVM (7) in the step (66). This value stored in the non-volatile memory (7) is intended to be used later. The secondary program, in the step 67, then extracts n high-order or low-order bits in R10 in order to obtain a value r which will make it possible to indicate which program sequence among the secondary program sequences (61, 62, 63, . . . , 6n) is to be executed. Each secondary program sequence will produce a different process: for example, the sequence (0) is comprised, first of all, of the step 611 for transferring the content of the register R11 of the microprocessor into a register R12. In the step 612, the content of R12 is added to the carry value (CARRY), then in the step 613, an exclusive OR is executed between the content of the register R11 and the content of the register R12, and the result is placed in the register R12. In the step 614, the processor decrements R12; in the step 615, a test is carried out on the value of R12 to determine whether or not R12 is equal to zero. In the case where R12=0, the processor returns to the execution of the main program. In the opposite case, in the step 616, the secondary program (61) executes a rotation of the content of the register R10. The next step consists of extracting n bits of a determined order from the register R10, in order to then access one of the sequences determined by this value r in the secondary program. Thus, it is possible to access, for example, the sequence (2^{n-1}) which, in the step (6n1), is comprised

	of transferring the result of the multiplication of the values of R10 and R11 into R13 and R14. In the step (6n2), this sequence executes a rotation of R13 and R14, then, in the step (6n3), the content of R13 is transferred into R11. In the step (6n4), R11 is decremented in order to then, in the step (6n5), perform a test on the value R11. This test is comprised of determining whether or not the content of R11=3. If so, the process returns to the main program and if not, the program proceeds to the step (6n6) by rotating R10 to the left, then executing the instruction (67) in order to access a new secondary program sequence." 6:44-65 – "In the case where the secondary program is intended to be combined with a decorrelated clock or interrupt handlers, it is possible in a combination of this type to restrict oneself to one secondary program, thus producing a simpler process. A simplified secondary program of this type can be constituted by the following instructions: MOV B, R2 which is comprised of loading the register R2 into the microprocessor register B LOOP DCX B which is comprised of decrementing the register B with the value A JNZ B LOOP which is comprised of performing a test on the value of the register B and of looping back to the label LOOP if this value is different from zero. This sequence ends with an instruction to return to the instruction of the main program which immediately follows the last instruction executed before the jump to the secondary program (6). The register R2 is pre-loaded by an instruction of the main program (5), before the jump to the secondary program (6), with a random value supplied by the random number generator (2). Thus, the execution of the secondary program defined above will always generate a variable duration." Figure 1.
(b) program logic to transmit said unpredictable information to an additional power expending circuit contained in said microchip.	Figure 1.

Claim 9 ('661 Patent)	U.S. 5,944,833 to Ugon
A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring, comprising:	Abstract – "The present invention relates to an improved integrated circuit for a microprocessor controlled by at least one program and the process for using the circuit which includes means which can decorrelate the running of at least one instruction sequence of a program from internal or external electrical signals of the integrated circuit." 1:44-60 – "This capability of being able to observe the running of a program in a microprocessor or a microcomputer is a major drawback when the microprocessor or microcomputer is used in high-security applications. In effect, an ill-intentioned individual would thus be able to know the successive states of the processor and use this information to gain knowledge of certain internal output data. It is possible to imagine, for example, that a given action on an external signal could take place at different instants as a function of the result of a determined security operation, such as the testing of confidential internal information or the decryption of a message, or even the integrity checking of certain information. Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used." 1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 2:2-7 – "One of the objects of the invention is to equip the circuit with means for preventing the type of investigation described above, and more generally for preventing observations, whether illicit or not, of the internal behavior of the circuit." 2:8-11 – "This object is achieved through the fact that the improved integrated circuit has means for decorrelating the running of at least one instruction sequence of a program from the internal or external signals of the circuit." 2:12-13 – "According to another characteristic, the electrical signals of the circuit are timing, synchronization or status signals." 3:59-63 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as

	mentioned above, are particularly known through the ST16XY family of microcomputers." Claim 1 – "A process including a main program having interrupt sequences arranged to execute at least one operation and at least one instruction sequence in a microprocessor in synchronization with internal or external electrical signals of an integrated circuit comprising means for decorrelating an execution of the at least one instruction sequence of the program from the internal or external electrical signals of the integrated circuit so that the execution of the at least one instruction sequence is desynchronized with respect to the internal or external electrical signals . . . ."
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	1:44-60 – "This capability of being able to observe the running of a program in a microprocessor or a microcomputer is a major drawback when the microprocessor or microcomputer is used in high-security applications. In effect, an ill-intentioned individual would thus be able to know the successive states of the processor and use this information to gain knowledge of certain internal output data. It is possible to imagine, for example, that a given action on an external signal could take place at different instants as a function of the result of a determined security operation, such as the testing of confidential internal information or the decryption of a message, or even the integrity checking of certain information. Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used." 1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 3:51-58 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories." 3:59-4:3 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family

	of microcomputers. However, these microcomputers or microprocessors, which use a shift register with parallel input-outputs looped back to at least one of its inputs, wherein the shift is timed by an internal clock, to constitute the random number generator, use the external clock for sequencing the machine cycles of the microprocessor to execute the instruction to read the contents of the register." 4:40-44 – "In the invention, the random number generator (2) is used either to supply a random value to the various devices through the data bus (3) and load it into the various devices which will be described below, or to generate a pulse signal of variable periodicity at its output (22)." *See also* Figures 1, 2 (*e.g.*, element 3). Claim 7 – "The integrated circuit according to claim 4, characterized in that said integrated circuit includes logic circuits and connecting busses connected such that sequencing of operations of the microprocessor factors in times required to access logic circuits of the integrated circuit, including signal propagation times in the busses and through the logic circuits." *See also* U.S. Patent No. 5,068,894 (Issued Nov. 26, 1991) at, *e.g.*, 5:4-29.
(b) a source of unpredictable information;	2:8-11 – "This object is achieved through the fact that the improved integrated circuit has means for decorrelating the running of at least one instruction sequence of a program from the internal or external signals of the circuit." 2:14-34 – "According to another characteristic, the decorrelation means comprise one or more circuits generating a sequence of clock or timing pulses which are dispatched at random times. According to another characteristic, the decorrelation means comprise a random number generator which makes it possible to de-synchronize the execution of the program sequence in the processor . . . . According to another characteristic, the decorrelation means comprise a random interrupt generating system. According to another characteristic, the decorrelation means comprise the execution of secondary sequences in which the instructions and execution times are different and which are selected at random. According to another characteristic, the variable time of the secondary process depends on a value supplied by a random number generator." 3:59-61 – "The invention will now be explained with the aid of FIG. 1

	in which a CPU (1) comprises a random number generator (2) . . . ." 4:40-48 – "In the invention, the random number generator (2) is used either to supply a random value to the various devices through the data bus (3) and load it into the various devices which will be described below, or to generate a pulse signal of variable periodicity at its output (22). In a microprocessor or microcomputer of the invention, the signals required for the loading and execution of the instructions can therefore be generated from randomly dispatched clock pulses . . . ." 9:55-10:20 – "For the random number generator (2), it is possible, for example, to use looped counters having different periods, which counters are initialized with a 'seed' (information) stored in a non-volatile memory (7). When the processor starts up, the counters factor in the stored value as the initial value. During the calculation, or at the end of the calculation, the non-volatile memory (7) is updated with a new value which will serve as a seed for initializing the counters at the next initialization. The interrupt generating circuit (4) can be designed so that the generation of interrupt pulses seen above can occur, for example, when the number generated has certain characteristics, such as equality with certain data of the program. This circuit (4) can also take on the value of one or more bits of one or more counters. It is also possible to produce a very good random number generator using a cryptographic algorithm (69), as shown in FIG. 5 or a hash function initialized by the 'seeds' (information) seen above. In this case, the generator can be in the form of a program which implements the algorithm executed by the processor (1) and which, for example, implements the cryptographic algorithm by receiving a variable stored in the non-volatile memory (7) and a key for generating an output stored in a buffer register (41). This output stored in the buffer register is then processed by a hardware or software decoding device (42) for generating either the decorrelated clock signal (IT) CLK2 or a signal for interrupting the processor (1). It is easy to see that this random number generator can also be used to generate the various random numbers seen above. Another way to produce a generator of this type is to amplify the voltage generated at the terminals of a so-called 'noise' diode and to shape the signals after a low pass filtering for preventing the noise pulses that are too rapid from disturbing the operation." Figures 1, 2, 4A, 7A, 7B. *See also* 2:48-50, 2:55-57, 2:63-65, 8:39-52.
(c) a processor:	3:51-58 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated

	with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories." 3:59-61 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) . . . ." Figures 1, 2.
(i) connected to said input interface for receiving and cryptographically processing said quantity,	1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 3:51-58 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories." 3:59-4:3 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers. However, these microcomputers or microprocessors, which use a shift register with parallel input-outputs looped back to at least one of its inputs, wherein the shift is timed by an internal clock, to constitute the random number generator, use the external clock for sequencing the machine cycles of the microprocessor to execute the instruction to read the contents of the register."
(ii) configured to use said unpredictable information to conceal a correlation between externally monitorable signals and said secret during said	2:28-31 – "According to another characteristic, the decorrelation means comprise the execution of secondary sequences in which the instructions and execution times are different and which are selected at random." 5:46-67 – "Lastly, the device of the invention can also comprise a secondary program (6) which, as will be seen below, can generate a variable duration time which varies each time this secondary program (6) is called by the main program (5). Thus, the variant of embodiment represented in FIG. 1 allows the main program (5) to change the

processing of said quantity;	desired degrees of protection, either by triggering the sequencing of the execution of one or more instructions with the aid of the decorrelated clock CLK2, or by deciding during the execution of an instruction sequence to introduce, or not to introduce, a randomly triggered interrupt handler, or by deciding during the execution of the sequence to introduce, or not to introduce, a jump to the secondary program (6), which also generates a process with a variable time, or even by combining these various possibilities. Thus, in a variant of the invention, this secondary program (6) can be constituted as represented in FIG. 8 by a plurality of sequences (61, 62, 63 . . . 6n) which are called at random; and each sequence (0, 1, 2 or 2^{n-1}) will implement a different set of instructions which will result in a variable processing time in each branch and different behaviors of the microprocessor." 8:31-36 – "It is also possible to produce a fifth simplified embodiment of the invention which does not use an interrupt. When the main program needs to be protected, it independently activates a secondary program, which generates a process of random length at instants it selects, either at the start or during execution, so as to scramble the various sequences." 9:38-54 – "It may also be seen that no matter what the variant of embodiment, the running of the main program occurs with an unpredictable sequencing which, depending on the variant, depends on the random number generator, on the random clock, on the secondary program, on the random interrupts, or on a combination of at least two of these devices. When the main program executes functions that are not sensitive from the point of view of security, it can also return to the external clock CLKE, for example in order to deliver output data to the external world or to mask the decorrelation interrupt in order to optimize the processing time. As soon as a security function is implemented, the main program (5) authorizes the random mode of operation by validating either the random clock or the decorrelation interrupt (or both) in order to 'scramble' the various operational signals, particularly by de-synchronizing the clock relative to the main program, or by calling the secondary program." Claim 1 – "A process including a main program having interrupt sequences arranged to execute at least one operation and at least one instruction sequence in a microprocessor in synchronization with internal or external electrical signals of an integrated circuit comprising means for decorrelating an execution of the at least one instruction sequence of the program from the internal or external electrical signals of the integrated circuit so that the execution of the at least one instruction sequence is desynchronized with respect to the internal or external electrical signals, characterized in that the process

	comprises at least one of the following steps: a) triggering the sequencing of one of at least one instruction or at least one operation with the aid of a random-pulse clock; b) randomly triggering the interrupt sequences; c) triggering the processing of a random sequence of instructions or operations during the execution of a main sequence of instructions or operations; d) combining at least two of steps a, b and c." Claim 8 – "The integrated circuit according to claim 4, characterized in that the decorrelation means comprises means for execution of a secondary program, the secondary program including a random choice of one of a plurality of sequences, the plurality of sequences including sequences each having a different set of instructions and a different execution time than all other ones of the plurality of sequences." Claim 9 – "The integrated circuit according to claim 8, characterized in that the secondary program sequence generates a variable duration, wherein the variable duration depends on a value supplied by a random number generator."
(d) an output interface for outputting said cryptographically processed quantity to a recipient thereof;	1:51-67 – "It is possible to imagine, for example, that a given action on an external signal could take place at different instants as a function of the result of a determined security operation, such as the testing of confidential internal information or the decryption of a message, or even the integrity checking of certain information. Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used. Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 3:51-4:3 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories. The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers. However, these microcomputers or microprocessors, which use a shift register

	with parallel input-outputs looped back to at least one of its inputs, wherein the shift is timed by an internal clock, to constitute the random number generator, use the external clock for sequencing the machine cycles of the microprocessor to execute the instruction to read the contents of the register." *See also* Figures 1, 2 (*e.g.*, element 3). Claim 7 – "The integrated circuit according to claim 4, characterized in that said integrated circuit includes logic circuits and connecting busses connected such that sequencing of operations of the microprocessor factors in times required to access logic circuits of the integrated circuit, including signal propagation times in the busses and through the logic circuits." *See also* U.S. Patent No. 5,068,894 (Issued Nov. 26, 1991) at, *e.g.*, 5:4-29.
(e) a hardware-implemented noise production subunit connected to said source of unpredictable information and configured to expend unpredictable amounts of electricity based on the output of said source of unpredictable information; and	4:40-5:19 -- "In the invention, the random number generator (2) is used either to supply a random value to the various devices through the data bus (3) and load it into the various devices which will be described below, or to generate a pulse signal of variable periodicity at its output (22). In a microprocessor or microcomputer of the invention, the signals required for the loading and execution of the instructions can therefore be generated from randomly dispatched clock pulses, but these pulses must adhere to a minimum cycle time so that the processor (1) has enough time to execute the various operations. This signal, in order to serve as a clock for the microprocessor (1), must be sent to a calibration circuit (9). The output (95) of this calibration circuit is sent to a multiplexing circuit (18) whose input (19) for controlling the multiplexing receives the signal of one or more bits of a register (8) which can be loaded either by the random number generator (2) or with a value determined by the main program (5). When this register (8) is loaded with a random value, the decision which selects the clock signal sent to the processor is made randomly, whereas when this register (8) is loaded with a value determined by the main program, it is the main program which will choose whether the clock for sequencing the microprocessor will be the external clock CLKE or a decorrelation clock CLK2. Likewise, one or more bits of the register (8) are sent through the link (82) to a logic circuit (28) which makes it possible, as a function of the bit or bits of the register (8), to validate or not to validate the transmission of the internal clock signal (11) to the random number generator (2). This random number generator can then also run on the external clock CLKE by receiving its signal through the link (26) and the logic circuit (28). In this latter case, the values generated will be pseudo-random values. The random number generator (2) can operate using

	the internal clock (11) validated through the circuit (28) by the bit or bits of the register (8), and in this case, the values generated will be random values. The signal I generated at the output (22) of the random number generator (2) and received by the calibration circuit (9) corresponds to a pulse signal whose periodicity varies, either randomly or in pseudo-random fashion. The fact that this periodicity varies in pseudo-random fashion is of little concern since, as will be seen below, the calibration circuit (9) introduces an internal clock signal (FRC) which will itself reintroduce a decorrelation, through a different frequency and a phase shift relative to the external clock signal CLKE, and consequently relative to the pseudo-random clock signal synchronized to this external clock signal." 7:45-65 – "In another embodiment, it is possible to introduce a variable phase shifting circuit (45) at the output of the clock circuit, as shown in FIG. 4A, which phase shifting circuit is constituted for example by a shift registers D1 through D5 timed by the signal FRC issuing from the clock circuit (11) or the recalibrated FRC supplied by the output (95) of the circuit (9) and phase shifting the signal I supplied by the output (22), which can be divided by a slowdown factor in a divisor (452). The output of the phase shifting circuit (45) can be produced with the aid of a multiplexer (451) MUX which makes it possible to extract any of the output signals Q1, Q2, . . . , Q5 from the shift register as a function of the content of the register RM which is loaded, either directly by the random number generator (2), or indirectly by the main program (5) or even by the secondary program (6), through the bus (3). In this case, the clock leading edges S delivered as output can be delayed or advanced relative to a median pulse supplied by the central level of the shift register, by a value which depends on a random number, thus proportionally delaying or advancing the instruction execution sequencing of the program in progress." Figures 3A, 4A.
(f) an activation controller, which may be activated by software contained in said device, to activate and deactivate said expending of unpredictable amounts of electricity.	2:43-44 – "According to another characteristic, the main program can enable or disable one or more decorrelation means." 5:20-45 – "The device can also comprise a register R2 which is loaded, either by the random number generator (2) with a random number, or by the main program (5) with a value determined by the program. This register R2 is totally or partially used by a logic circuit (4) for triggering an interrupt, which receives at one of its inputs the decorrelated clock signal CLK2 issuing from the output (95) of the calibration circuit (9). The output of the circuit (4) is sent through a gate (48) controlled by one or more bits of the register (8) to the interrupt input (12) of the CPU. The bit or bits of this register (8) play

	the role of an interrupt mask control, which is standard in certain microprocessors. When an interrupt is received at the interrupt input (12) of the processor, the interrupt handling program contained, for example, in the operating system or in the secondary program will introduce a different processing time for the interrupted sequence of the main program. It must be understood that there are two phases in the interrupt mode of operation. A first phase, in which the microprocessor controlled by the so-called main program authorizes the decorrelated operation by unmasking, for example, the interrupts. A second phase, in which the interrupt automatically reroutes the operation to the secondary program. This operation can actually occur without the intervention of the main program." 5:46-60 – "Lastly, the device of the invention can also comprise a secondary program (6) which, as will be seen below, can generate a variable duration time which varies each time this secondary program (6) is called by the main program (5). Thus, the variant of embodiment represented in FIG. 1 allows the main program (5) to change the desired degrees of protection, either by triggering the sequencing of the execution of one or more instructions with the aid of the decorrelated clock CLK2, or by deciding during the execution of an instruction sequence to introduce, or not to introduce, a randomly triggered interrupt handler, or by deciding during the execution of the sequence to introduce, or not to introduce, a jump to the secondary program (6), which also generates a process with a variable time, or even by combining these various possibilities." 7:13-26 – "The execution of this instruction of the main program (5) therefore causes the addressing by the processor (1), at random, of instructions whose execution durations will be different depending on the position addressed. In a known way, the random number generator (2) will be initialized at the start to a variable. This initial variable is contained in a non-volatile memory (7) and constituted, for example, by the last random value generated by the generator (2) before the pausing of the microprocessor (1). Thus, the microprocessor, controlled by a program it will execute, will be able to use this program to activate the means for decorrelating the instruction execution sequencing of this program by loading, for example, registers R2 or 8, or by calling secondary programs." 8:31-36 – "It is also possible to produce a fifth simplified embodiment of the invention which does not use an interrupt. When the main program needs to be protected, it independently activates a secondary program, which generates a process of random length at instants it selects, either at the start or during execution, so as to scramble the various sequences."

	Claim 12 – "The integrated circuit according to claim 4, characterized in that the main program can enable or disable the decorrelation means."

Claim 10 ('661 Patent)	**U.S. 5,944,833 to Ugon**
The device of claim 9 wherein said source of unpredictable information is a hardware-implemented random number generator, and wherein said noise production subunit includes a digital-to-analog converter.	2:32-34 – "According to another characteristic, the variable time of the secondary process depends on a value supplied by a random number generator." 4:9-11 – "The invention is comprised of using the principle of a microprocessor of this type with a random number generator . . . ." 4:40-44 – "In the invention, the random number generator (2) is used either to supply a random value to the various devices through the data bus (3) and load it into the various devices which will be described below, or to generate a pulse signal of variable periodicity at its output (22).: 5:5-12 – "The random number generator (2) can operate using the internal clock (11) validated through the circuit (28) by the bit or bits of the register (8), and in this case, the values generated will be random values. The signal I generated at the output (22) of the random number generator (2) and received by the calibration circuit (9) corresponds to a pulse signal whose periodicity varies, either randomly or in pseudo-random fashion." 10:1-13 – "It is also possible to produce a very good random number generator using a cryptographic algorithm (69), as shown in FIG. 5 or a hash function initialized by the 'seeds' (information) seen above. In this case, the generator can be in the form of a program which implements the algorithm executed by the processor (1) and which, for example, implements the cryptographic algorithm by receiving a variable stored in the non-volatile memory (7) and a key for generating an output stored in a buffer register (41). This output stored in the buffer register is then processed by a hardware or software decoding device (42) for generating either the decorrelated clock signal (IT) CLK2 or a signal for interrupting the processor (1)." Claim 5 – "The integrated circuit according to claim 4, characterized in that the decorrelation means comprises at least one circuit for generating a sequence of timing pulses which are dispatched at random times to the microprocessor by generation of a random

	number." Figures 5, 7A. *See also* 8:39-9:27. *See also, e.g.,* English abstracts of JP10084223, JP10197610, JP62260406, and JP62082702 (describing including a digital to analog converter in a noise production subunit).

Claim 11 ('661 Patent)	**U.S. 5,944,833 to Ugon**
A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external measurement of said device's power consumption, comprising:	Abstract – "The present invention relates to an improved integrated circuit for a microprocessor controlled by at least one program and the process for using the circuit which includes means which can decorrelate the running of at least one instruction sequence of a program from internal or external electrical signals of the integrated circuit." 1:44-60 – "This capability of being able to observe the running of a program in a microprocessor or a microcomputer is a major drawback when the microprocessor or microcomputer is used in high-security applications. In effect, an ill-intentioned individual would thus be able to know the successive states of the processor and use this information to gain knowledge of certain internal output data. It is possible to imagine, for example, that a given action on an external signal could take place at different instants as a function of the result of a determined security operation, such as the testing of confidential internal information or the decryption of a message, or even the integrity checking of certain information. Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used." 1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 2:2-7 – "One of the objects of the invention is to equip the circuit with means for preventing the type of investigation described above, and more generally for preventing observations, whether illicit or not, of

	the internal behavior of the circuit." 2:8-11 – "This object is achieved through the fact that the improved integrated circuit has means for decorrelating the running of at least one instruction sequence of a program from the internal or external signals of the circuit." 2:12-13 – "According to another characteristic, the electrical signals of the circuit are timing, synchronization or status signals." 3:59-63 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers." Claim 1 – "A process including a main program having interrupt sequences arranged to execute at least one operation and at least one instruction sequence in a microprocessor in synchronization with internal or external electrical signals of an integrated circuit comprising means for decorrelating an execution of the at least one instruction sequence of the program from the internal or external electrical signals of the integrated circuit so that the execution of the at least one instruction sequence is desynchronized with respect to the internal or external electrical signals . . . ."
(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	1:44-60 – "This capability of being able to observe the running of a program in a microprocessor or a microcomputer is a major drawback when the microprocessor or microcomputer is used in high-security applications. In effect, an ill-intentioned individual would thus be able to know the successive states of the processor and use this information to gain knowledge of certain internal output data. It is possible to imagine, for example, that a given action on an external signal could take place at different instants as a function of the result of a determined security operation, such as the testing of confidential internal information or the decryption of a message, or even the integrity checking of certain information. Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used." 1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for

	example, for the calculation of encryptions and decryptions." 3:51-58 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories." 3:59-4:3 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers. However, these microcomputers or microprocessors, which use a shift register with parallel input-outputs looped back to at least one of its inputs, wherein the shift is timed by an internal clock, to constitute the random number generator, use the external clock for sequencing the machine cycles of the microprocessor to execute the instruction to read the contents of the register." 4:40-44 – "In the invention, the random number generator (2) is used either to supply a random value to the various devices through the data bus (3) and load it into the various devices which will be described below, or to generate a pulse signal of variable periodicity at its output (22)." *See also* Figures 1, 2 (*e.g.*, element 3). Claim 7 – "The integrated circuit according to claim 4, characterized in that said integrated circuit includes logic circuits and connecting busses connected such that sequencing of operations of the microprocessor factors in times required to access logic circuits of the integrated circuit, including signal propagation times in the busses and through the logic circuits." *See also* U.S. Patent No. 5,068,894 (Issued Nov. 26, 1991) at, *e.g.*, 5:4-29.
(b) an input interface for receiving a variable amount of power, said power consumption varying measurably during said performance of	1:44-60 – "This capability of being able to observe the running of a program in a microprocessor or a microcomputer is a major drawback when the microprocessor or microcomputer is used in high-security applications. In effect, an ill-intentioned individual would thus be able to know the successive states of the processor and use this information to gain knowledge of certain internal output data. It is possible to imagine, for example, that a given action on an external signal could

said operation;	take place at different instants as a function of the result of a determined security operation, such as the testing of confidential internal information or the decryption of a message, or even the integrity checking of certain information. Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used." 1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 2:8-13 – "This object is achieved through the fact that the improved integrated circuit has means for decorrelating the running of at least one instruction sequence of a program from the internal or external signals of the circuit. According to another characteristic, the electrical signals of the circuit are timing, synchronization or status signals." 3:51-58 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories." 3:59-63 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers." Claim 2 – "An integrated circuit comprising a microprocessor controlled by at least one program including at least one program interrupt, the at least one program being arranged to execute at least one instruction sequence in the microprocessor in synchronization with internal or external electrical signals of the integrated circuit and means for decorrelating execution of the at least one instruction sequence of the program from the internal or external electrical signals of the integrated circuit so that the execution of the at least one instruction sequence is desynchronized with respect to the internal or external electrical signals and the program having an instruction sequence for authorization, modification, or disablement of the

	decorrelation means, wherein authorization includes unmasking the program interrupts." Abstract – "The present invention relates to an improved integrated circuit for a microprocessor controlled by at least one program and the process for using the circuit which includes means which can decorrelate the running of at least one instruction sequence of a program from internal or external electrical signals of the integrated circuit." *See also* U.S. Patent No. 5,068,894 (Issued Nov. 26, 1991) at, *e.g.*, 5:4-29.
(c) a processor connected to said input interface for receiving and cryptographically processing said quantity; and	1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 3:51-58 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories." 3:59-63 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers." Figures 1, 2.
(d) a noise production system for introducing noise into said measurement of said power consumption.	Abstract – "The present invention relates to an improved integrated circuit for a microprocessor controlled by at least one program and the process for using the circuit which includes means which can decorrelate the running of at least one instruction sequence of a program from internal or external electrical signals of the integrated circuit." 3:59-61 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) . . . ." 2:14-34 – "According to another characteristic, the decorrelation

	means comprise one or more circuits generating a sequence of clock or timing pulses which are dispatched at random times. According to another characteristic, the decorrelation means comprise a random number generator which makes it possible to de-synchronize the execution of the program sequence in the processor . . . . According to another characteristic, the decorrelation means comprise a random interrupt generating system. According to another characteristic, the decorrelation means comprise the execution of secondary sequences in which the instructions and execution times are different and which are selected at random. According to another characteristic, the variable time of the secondary process depends on a value supplied by a random number generator." 4:40-48 – "In the invention, the random number generator (2) is used either to supply a random value to the various devices through the data bus (3) and load it into the various devices which will be described below, or to generate a pulse signal of variable periodicity at its output (22). In a microprocessor or microcomputer of the invention, the signals required for the loading and execution of the instructions can therefore be generated from randomly dispatched clock pulses . . . ." Claim 1 – "A process including a main program having interrupt sequences arranged to execute at least one operation and at least one instruction sequence in a microprocessor in synchronization with internal or external electrical signals of an integrated circuit comprising means for decorrelating an execution of the at least one instruction sequence of the program from the internal or external electrical signals of the integrated circuit so that the execution of the at least one instruction sequence is desynchronized with respect to the internal or external electrical signals, characterized in that the process comprises at least one of the following steps: a) triggering the sequencing of one of at least one instruction or at least one operation with the aid of a random-pulse clock; b) randomly triggering the interrupt sequences; c) triggering the processing of a random sequence of instructions or operations during the execution of a main sequence of instructions or operations; d) combining at least two of steps a, b and c." Claim 2 – "An integrated circuit comprising a microprocessor controlled by at least one program including at least one program interrupt, the at least one program being arranged to execute at least one instruction sequence in the microprocessor in synchronization with internal or external electrical signals of the integrated circuit and means for decorrelating execution of the at least one instruction sequence of the program from the internal or external electrical signals of the integrated circuit so that the execution of the at least one instruction sequence is desynchronized with respect to the internal or

	external electrical signals and the program having an instruction sequence for authorization, modification, or disablement of the decorrelation means, wherein authorization includes unmasking the program interrupts."

Claim 12 ('661 Patent)	**U.S. 5,944,833 to Ugon**
The device of claim 11 wherein said noise production system comprises: (a) a source of randomness for generating initial noise having a random characteristic;	4:40-44 – "In the invention, the random number generator (2) is used either to supply a random value to the various devices through the data bus (3) and load it into the various devices which will be described below, or to generate a pulse signal of variable periodicity at its output (22)." 9:55-10:20 – "For the random number generator (2), it is possible, for example, to use looped counters having different periods, which counters are initialized with a 'seed' (information) stored in a non-volatile memory (7). When the processor starts up, the counters factor in the stored value as the initial value. During the calculation, or at the end of the calculation, the non-volatile memory (7) is updated with a new value which will serve as a seed for initializing the counters at the next initialization. The interrupt generating circuit (4) can be designed so that the generation of interrupt pulses seen above can occur, for example, when the number generated has certain characteristics, such as equality with certain data of the program. This circuit (4) can also take on the value of one or more bits of one or more counters. It is also possible to produce a very good random number generator using a cryptographic algorithm (69), as shown in FIG. 5 or a hash function initialized by the 'seeds' (information) seen above. In this case, the generator can be in the form of a program which implements the algorithm executed by the processor (1) and which, for example, implements the cryptographic algorithm by receiving a variable stored in the non-volatile memory (7) and a key for generating an output stored in a buffer register (41). This output stored in the buffer register is then processed by a hardware or software decoding device (42) for generating either the decorrelated clock signal (IT) CLK2 or a signal for interrupting the processor (1). It is easy to see that this random number generator can also be used to generate the various random numbers seen above. Another way to produce a generator of this type is to amplify the voltage generated at the terminals of a so-called 'noise' diode and to shape the signals after a low pass filtering for preventing the noise pulses that are too rapid from disturbing the operation."
(b) a noise processing	5:46-60 – "Lastly, the device of the invention can also comprise a

module for improving the random characteristic of said initial noise; and	secondary program (6) which, as will be seen below, can generate a variable duration time which varies each time this secondary program (6) is called by the main program (5). Thus, the variant of embodiment represented in FIG. 1 allows the main program (5) to change the desired degrees of protection, either by triggering the sequencing of the execution of one or more instructions with the aid of the decorrelated clock CLK2, or by deciding during the execution of an instruction sequence to introduce, or not to introduce, a randomly triggered interrupt handler, or by deciding during the execution of the sequence to introduce, or not to introduce, a jump to the secondary program (6), which also generates a process with a variable time, or even by combining these various possibilities." 10:15-20 – "Another way to produce a generator of this type is to amplify the voltage generated at the terminals of a so-called 'noise' diode and to shape the signals after a low pass filtering for preventing the noise pulses that are too rapid from disturbing the operation." Claim 1 – "A process including a main program having interrupt sequences arranged to execute at least one operation and at least one instruction sequence in a microprocessor in synchronization with internal or external electrical signals of an integrated circuit comprising means for decorrelating an execution of the at least one instruction sequence of the program from the internal or external electrical signals of the integrated circuit so that the execution of the at least one instruction sequence is desynchronized with respect to the internal or external electrical signals, characterized in that the process comprises at least one of the following steps: a) triggering the sequencing of one of at least one instruction or at least one operation with the aid of a random-pulse clock; b) randomly triggering the interrupt sequences; c) triggering the processing of a random sequence of instructions or operations during the execution of a main sequence of instructions or operations; d) combining at least two of steps a, b and c." Claim 3 – "An integrated circuit according to claim 2, characterized in that the decorrelation means comprises means for generating one of a timing signal, and a sequence of clock pulses which is dispatched at random times, and used to sequence one of means for randomly generating interrupts and means for triggering the execution of a secondary sequence."
(c) a noise production module configured to vary said power consumption based on an output of said noise	5:60-66 – "Thus, in a variant of the invention, this secondary program (6) can be constituted as represented in FIG. 8 by a plurality of sequences (61, 62, 63 . . . 6n) which are called at random; and each sequence (0, 1, 2 or 2^{n-1}) will implement a different set of instructions which will result in a variable processing time in each branch and

processing module.	different behaviors of the microprocessor." 6:66-7:18 – "Another embodiment of a secondary program of variable duration can be comprised of defining an area of the program storage corresponding to the secondary program (6) in which a set of instructions is stored. Preferably, the instructions chosen require different numbers of machine cycles in order to be executed, as is known to be the case, for example, with the instructions J, CALL, RET, RST, PCHL, INX in relation to instructions requiring a number of shorter machine cycles such as ADC, SUB, ANA, MOV, etc. Thus, in this storage area, there are a certain number of available instructions having execution durations that are different from one another in terms of the number of machine cycles. The main program (5) comprises an instruction to jump to an indexed address whose index corresponds to the content of the register R2 and whose address corresponds to the first address of the area (6). The execution of this instruction of the main program (5) therefore causes the addressing by the processor (1), at random, of instructions whose execution durations will be different depending on the position addressed. In a known way, the random number generator (2) will be initialized at the start to a variable." 9:37-40 – "It may also be seen that no matter what the variant of embodiment, the running of the main program occurs with an unpredictable sequencing which, depending on the variant, depends on the random number generator, on the random clock, on the secondary program, on the random interrupts, or on a combination of at least two of these devices."

Claim 13 ('661 Patent)	**U.S. 5,944,833 to Ugon**
The device of claim 12 wherein said noise production system is connected to said processor and is selectively operable under the control of said processor.	2:43-44 – "According to another characteristic, the main program can enable or disable one or more decorrelation means." 5:20-45 – "The device can also comprise a register R2 which is loaded, either by the random number generator (2) with a random number, or by the main program (5) with a value determined by the program. This register R2 is totally or partially used by a logic circuit (4) for triggering an interrupt, which receives at one of its inputs the decorrelated clock signal CLK2 issuing from the output (95) of the calibration circuit (9). The output of the circuit (4) is sent through a gate (48) controlled by one or more bits of the register (8) to the interrupt input (12) of the CPU. The bit or bits of this register (8) play the role of an interrupt mask control, which is standard in certain

	microprocessors. When an interrupt is received at the interrupt input (12) of the processor, the interrupt handling program contained, for example, in the operating system or in the secondary program will introduce a different processing time for the interrupted sequence of the main program. It must be understood that there are two phases in the interrupt mode of operation. A first phase, in which the microprocessor controlled by the so-called main program authorizes the decorrelated operation by unmasking, for example, the interrupts. A second phase, in which the interrupt automatically reroutes the operation to the secondary program. This operation can actually occur without the intervention of the main program." 5:46-60 – "Lastly, the device of the invention can also comprise a secondary program (6) which, as will be seen below, can generate a variable duration time which varies each time this secondary program (6) is called by the main program (5). Thus, the variant of embodiment represented in FIG. 1 allows the main program (5) to change the desired degrees of protection, either by triggering the sequencing of the execution of one or more instructions with the aid of the decorrelated clock CLK2, or by deciding during the execution of an instruction sequence to introduce, or not to introduce, a randomly triggered interrupt handler, or by deciding during the execution of the sequence to introduce, or not to introduce, a jump to the secondary program (6), which also generates a process with a variable time, or even by combining these various possibilities." 7:13-26 – "The execution of this instruction of the main program (5) therefore causes the addressing by the processor (1), at random, of instructions whose execution durations will be different depending on the position addressed. In a known way, the random number generator (2) will be initialized at the start to a variable. This initial variable is contained in a non-volatile memory (7) and constituted, for example, by the last random value generated by the generator (2) before the pausing of the microprocessor (1). Thus, the microprocessor, controlled by a program it will execute, will be able to use this program to activate the means for decorrelating the instruction execution sequencing of this program by loading, for example, registers R2 or 8, or by calling secondary programs." 8:31-36 – "It is also possible to produce a fifth simplified embodiment of the invention which does not use an interrupt. When the main program needs to be protected, it independently activates a secondary program, which generates a process of random length at instants it selects, either at the start or during execution, so as to scramble the various sequences." Claim 12 – "The integrated circuit according to claim 4, characterized

	in that the main program can enable or disable the decorrelation means."

Claim 14 ('661 Patent)	U.S. 5,944,833 to Ugon
A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring of said device's power consumption, comprising:	*See supra* disclosure regarding preamble of '661 patent claim 11.
(a) an input/output interface for receiving data to be cryptographically processed, said data being representative of at least a portion of a message;	*See supra* disclosure regarding '661 patent claim 1(a).
(b) an oscillator generating a first clock signal;	4:23-28 – "This is obtained by the circuit in FIG. 1 in which, in addition to the random number generator (2), the internal clock (11) is embodied by a free fixed frequency oscillator, de-synchronized and phase shifted relative to the external clock CLKE of the microprocessor or microcomputer."
(c) an input interface for receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	*See supra* disclosure regarding '661 patent claim 11(b).
(d) a source of unpredictable	*See supra* disclosure regarding '661 patent claim 1(b).

information;	
(e) a clock decorrelator coupled to said source of unpredictable information for generating a second clock signal from said first clock signal using said unpredictable information, such that said second clock signal cannot be reliably predicted from said first clock signal; and	4:40-63 – "In the invention, the random number generator (2) is used either to supply a random value to the various devices through the data bus (3) and load it into the various devices which will be described below, or to generate a pulse signal of variable periodicity at its output (22). In a microprocessor or microcomputer of the invention, the signals required for the loading and execution of the instructions can therefore be generated from randomly dispatched clock pulses, but these pulses must adhere to a minimum cycle time so that the processor (1) has enough time to execute the various operations. This signal, in order to serve as a clock for the microprocessor (1), must be sent to a calibration circuit (9). The output (95) of this calibration circuit is sent to a multiplexing circuit (18) whose input (19) for controlling the multiplexing receives the signal of one or more bits of a register (8) which can be loaded either by the random number generator (2) or with a value determined by the main program (5). When this register (8) is loaded with a random value, the decision which selects the clock signal sent to the processor is made randomly, whereas when this register (8) is loaded with a value determined by the main program, it is the main program which will choose whether the clock for sequencing the microprocessor will be the external clock CLKE or a decorrelation clock CLK2." 5:5-12 – "The random number generator (2) can operate using the internal clock (11) validated through the circuit (28) by the bit or bits of the register (8), and in this case, the values generated will be random values. The signal I generated at the output (22) of the random number generator (2) and received by the calibration circuit (9) corresponds to a pulse signal whose periodicity varies, either randomly or in pseudo-random fashion." 10:1-15 – "It is also possible to produce a very good random number generator using a cryptographic algorithm (69), as shown in FIG. 5 or a hash function initialized by the 'seeds' (information) seen above. In this case, the generator can be in the form of a program which implements the algorithm executed by the processor (1) and which, for example, implements the cryptographic algorithm by receiving a variable stored in the non-volatile memory (7) and a key for generating an output stored in a buffer register (41). This output stored in the buffer register is then processed by a hardware or software decoding device (42) for generating either the decorrelated clock signal (IT) CLK2 or a signal for interrupting the processor (1). It is easy to see that this random number generator can also be used to generate the various random numbers seen above."

	Figures 1, 5. *See generally* 4:23-5:19.
(f) a processor:	*See supra* disclosure regarding '661 patent claim 1(c).
(i) clocked by said second clock signal,	4:57-63 – "When this register (8) is loaded with a random value, the decision which selects the clock signal sent to the processor is made randomly, whereas when this register (8) is loaded with a value determined by the main program, it is the main program which will choose whether the clock for sequencing the microprocessor will be the external clock CLKE or a decorrelation clock CLK2." Figure 1.
(ii) configured to cryptographically processing said data, and	1:51-67 – "It is possible to imagine, for example, that a given action on an external signal could take place at different instants as a function of the result of a determined security operation, such as the testing of confidential internal information or the decryption of a message, or even the integrity checking of certain information. Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used. Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions."
(iii) configured to output said cryptographically processed data using said input/output interface.	*See supra* disclosure regarding '661 patent claim 1(a).

Claim 15 ('661 Patent)	**U.S. 5,944,833 to Ugon**
A cryptographic processing device for securely performing a cryptographic processing operation in	Abstract – "The present invention relates to an improved integrated circuit for a microprocessor controlled by at least one program and the process for using the circuit which includes means which can decorrelate the running of at least one instruction sequence of a program from internal or external electrical signals of the integrated

a manner resistant to discovery of a secret by external monitoring of said device's power consumption, comprising:	circuit." 1:44-60 – "This capability of being able to observe the running of a program in a microprocessor or a microcomputer is a major drawback when the microprocessor or microcomputer is used in high-security applications. In effect, an ill-intentioned individual would thus be able to know the successive states of the processor and use this information to gain knowledge of certain internal output data. It is possible to imagine, for example, that a given action on an external signal could take place at different instants as a function of the result of a determined security operation, such as the testing of confidential internal information or the decryption of a message, or even the integrity checking of certain information. Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used." 1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 2:3-7 – "One of the objects of the invention is to equip the circuit with means for preventing the type of investigation described above, and more generally for preventing observations, whether illicit or not, of the internal behavior of the circuit." 2:8-11 – "This object is achieved through the fact that the improved integrated circuit has means for decorrelating the running of at least one instruction sequence of a program from the internal or external signals of the circuit." 2:12-13 – "According to another characteristic, the electrical signals of the circuit are timing, synchronization or status signals." 3:59-63 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers." Claim 1 – "A process including a main program having interrupt sequences arranged to execute at least one operation and at least one instruction sequence in a microprocessor in synchronization with internal or external electrical signals of an integrated circuit

	comprising means for decorrelating an execution of the at least one instruction sequence of the program from the internal or external electrical signals of the integrated circuit so that the execution of the at least one instruction sequence is desynchronized with respect to the internal or external electrical signals . . . ."
(a) an input/output interface for receiving data to be cryptographically processed, said data being representative of at least a portion of a message;	1:44-60 – "This capability of being able to observe the running of a program in a microprocessor or a microcomputer is a major drawback when the microprocessor or microcomputer is used in high-security applications. In effect, an ill-intentioned individual would thus be able to know the successive states of the processor and use this information to gain knowledge of certain internal output data. It is possible to imagine, for example, that a given action on an external signal could take place at different instants as a function of the result of a determined security operation, such as the testing of confidential internal information or the decryption of a message, or even the integrity checking of certain information. Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used." 1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 3:51-58 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories." 3:59-4:3 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers. However, these microcomputers or microprocessors, which use a shift register with parallel input-outputs looped back to at least one of its inputs, wherein the shift is timed by an internal clock, to constitute the random number generator, use the external clock for sequencing the machine cycles of the microprocessor to execute the instruction to read the contents of the

	register." 4:40-44 – "In the invention, the random number generator (2) is used either to supply a random value to the various devices through the data bus (3) and load it into the various devices which will be described below, or to generate a pulse signal of variable periodicity at its output (22)." *See also* Figures 1, 2 (*e.g.*, element 3). Claim 7 – "The integrated circuit according to claim 4, characterized in that said integrated circuit includes logic circuits and connecting busses connected such that sequencing of operations of the microprocessor factors in times required to access logic circuits of the integrated circuit, including signal propagation times in the busses and through the logic circuits." *See also* U.S. Patent No. 5,068,894 (Issued Nov. 26, 1991) at, *e.g.*, 5:4-29.
(b) an input interface for receiving an external clock signal;	4:57-63 – "When this register (8) is loaded with a random value, the decision which selects the clock signal sent to the processor is made randomly, whereas when this register (8) is loaded with a value determined by the main program, it is the main program which will choose whether the clock for sequencing the microprocessor will be the external clock CLKE or a decorrelation clock CLK2." 5:19-28 – "The device can also comprise a register R2 which is loaded, either by the random number generator (2) with a random number, or by the main program (5) with a value determined by the program. This register R2 is totally or partially used by a logic circuit (4) for triggering an interrupt, which receives at one of its inputs the decorrelated clock signal CLK2 issuing from the output (95) of the calibration circuit (9). The output of the circuit (4) is sent through a gate (48) controlled by one or more bits of the register (8) to the interrupt input (12) of the CPU." Figures 1, 2.
(c) an input interface for receiving a variable amount of power, said power consumption varying measurably during said performance of	1:44-60 – "This capability of being able to observe the running of a program in a microprocessor or a microcomputer is a major drawback when the microprocessor or microcomputer is used in high-security applications. In effect, an ill-intentioned individual would thus be able to know the successive states of the processor and use this information to gain knowledge of certain internal output data. It is possible to imagine, for example, that a given action on an external signal could take place at different instants as a function of the result

said operation;	of a determined security operation, such as the testing of confidential internal information or the decryption of a message, or even the integrity checking of certain information. Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used." 2:8-13 – "This object is achieved through the fact that the improved integrated circuit has means for decorrelating the running of at least one instruction sequence of a program from the internal or external signals of the circuit. According to another characteristic, the electrical signals of the circuit are timing, synchronization or status signals." 1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 3:51-58 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories." 3:59-63 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers." Claim 2 – "An integrated circuit comprising a microprocessor controlled by at least one program including at least one program interrupt, the at least one program being arranged to execute at least one instruction sequence in the microprocessor in synchronization with internal or external electrical signals of the integrated circuit and means for decorrelating execution of the at least one instruction sequence of the program from the internal or external electrical signals of the integrated circuit so that the execution of the at least one instruction sequence is desynchronized with respect to the internal or external electrical signals and the program having an instruction sequence for authorization, modification, or disablement of the decorrelation means, wherein authorization includes unmasking the

	program interrupts." Abstract – "The present invention relates to an improved integrated circuit for a microprocessor controlled by at least one program and the process for using the circuit which includes means which can decorrelate the running of at least one instruction sequence of a program from internal or external electrical signals of the integrated circuit." *See also* U.S. Patent No. 5,068,894 (Issued Nov. 26, 1991) at, *e.g.*, 5:4-29.
(d) a source of unpredictable information;	2:8-11 – "This object is achieved through the fact that the improved integrated circuit has means for decorrelating the running of at least one instruction sequence of a program from the internal or external signals of the circuit." 2:14-34 – "According to another characteristic, the decorrelation means comprise one or more circuits generating a sequence of clock or timing pulses which are dispatched at random times. According to another characteristic, the decorrelation means comprise a random number generator which makes it possible to de-synchronize the execution of the program sequence in the processor . . . . According to another characteristic, the decorrelation means comprise a random interrupt generating system. According to another characteristic, the decorrelation means comprise the execution of secondary sequences in which the instructions and execution times are different and which are selected at random. According to another characteristic, the variable time of the secondary process depends on a value supplied by a random number generator." 3:59-61 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) . . . ." 4:40-48 – "In the invention, the random number generator (2) is used either to supply a random value to the various devices through the data bus (3) and load it into the various devices which will be described below, or to generate a pulse signal of variable periodicity at its output (22). In a microprocessor or microcomputer of the invention, the signals required for the loading and execution of the instructions can therefore be generated from randomly dispatched clock pulses . . . ." 9:55-10:20 – "For the random number generator (2), it is possible, for example, to use looped counters having different periods, which counters are initialized with a 'seed' (information) stored in a non-volatile memory (7). When the processor starts up, the counters factor in the stored value as the initial value. During the calculation, or at the

	end of the calculation, the non-volatile memory (7) is updated with a new value which will serve as a seed for initializing the counters at the next initialization. The interrupt generating circuit (4) can be designed so that the generation of interrupt pulses seen above can occur, for example, when the number generated has certain characteristics, such as equality with certain data of the program. This circuit (4) can also take on the value of one or more bits of one or more counters. It is also possible to produce a very good random number generator using a cryptographic algorithm (69), as shown in FIG. 5 or a hash function initialized by the 'seeds' (information) seen above. In this case, the generator can be in the form of a program which implements the algorithm executed by the processor (1) and which, for example, implements the cryptographic algorithm by receiving a variable stored in the non-volatile memory (7) and a key for generating an output stored in a buffer register (41). This output stored in the buffer register is then processed by a hardware or software decoding device (42) for generating either the decorrelated clock signal (IT) CLK2 or a signal for interrupting the processor (1). It is easy to see that this random number generator can also be used to generate the various random numbers seen above. Another way to produce a generator of this type is to amplify the voltage generated at the terminals of a so-called 'noise' diode and to shape the signals after a low pass filtering for preventing the noise pulses that are too rapid from disturbing the operation." Figures 1, 2, 4A, 7A, 7B. *See also* 2:48-50, 2:55-57, 2:63-65, 8:39-52.
(e) a clock decorrelator coupled to said source of unpredictable information for generating an internal clock signal from said external clock signal using said unpredictable information, such that said internal clock signal cannot be reliably predicted from said external clock signal; and	4:57-63 – "It is the main program which will choose whether the clock for sequencing the microprocessor will be the external clock CLKE or a decorrelation clock CLK2" 5:1-19 – "This random number generator can then also run on the external clock CLKE by receiving its signal through the link (26) and the logic circuit (28). In this latter case, the values generated will be pseudo-random values . . . . The signal I generated at the output (22) of the random number generator (2) and received by the calibration circuit (9) corresponds to a pulse signal whose periodicity varies, either randomly or in pseudo-random fashion. The fact that this periodicity varies in pseudo-random fashion is of little concern since, as will be seen below, the calibration circuit (9) introduces an internal clock signal (FRC) which will itself reintroduce a decorrelation, through a different frequency and a phase shift relative to the external clock signal CLKE, and consequently relative to the pseudo-random clock signal synchronized to this external clock signal."

	Figure 1.
(f) a processor:	3:51-58 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories." 3:59-61 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) . . . ." Figures 1, 2.
(i) clocked by said internal clock signal,	4:57-63 – "It is the main program which will choose whether the clock for sequencing the microprocessor will be the external clock CLKE or a decorrelation clock CLK2" 5:1-19 – "This random number generator can then also run on the external clock CLKE by receiving its signal through the link (26) and the logic circuit (28). In this latter case, the values generated will be pseudo-random values . . . . The signal I generated at the output (22) of the random number generator (2) and received by the calibration circuit (9) corresponds to a pulse signal whose periodicity varies, either randomly or in pseudo-random fashion. The fact that this periodicity varies in pseudo-random fashion is of little concern since, as will be seen below, the calibration circuit (9) introduces an internal clock signal (FRC) which will itself reintroduce a decorrelation, through a different frequency and a phase shift relative to the external clock signal CLKE, and consequently relative to the pseudo-random clock signal synchronized to this external clock signal." Figure 1.
(ii) configured to cryptographically processing said data, and	3:51-58 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories." 3:59-61 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) . . . ." Figures 1, 2.

(iii) configured to output said cryptographically processed data using said input/output interface.	1:51-67 – "It is possible to imagine, for example, that a given action on an external signal could take place at different instants as a function of the result of a determined security operation, such as the testing of confidential internal information or the decryption of a message, or even the integrity checking of certain information. Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used. Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 3:51-58 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories." *See also* U.S. Patent No. 5,068,894 (Issued Nov. 26, 1991) at, *e.g.*, 5:4-29.

Claim 16 ('661 Patent)	**U.S. 5,944,833 to Ugon**
The device of claim 15 wherein said clock decorrelator comprises a clock skipping module which selects a subset of the cycles of said external clock signal to use as said internal clock signal based on said unpredictable information.	4:50-63 – "This signal, in order to serve as a clock for the microprocessor (1), must be sent to a calibration circuit (9). The output (95) of this calibration circuit is sent to a multiplexing circuit (18) whose input (19) for controlling the multiplexing receives the signal of one or more bits of a register (8) which can be loaded either by the random number generator (2) or with a value determined by the main program (5). When this register (8) is loaded with a random value, the decision which selects the clock signal sent to the processor is made randomly, whereas when this register (8) is loaded with a value determined by the main program, it is the main program which will choose whether the clock for sequencing the microprocessor will be the external clock CLKE or a decorrelation clock CLK2." *See also* U.S. Patent Number 5,404,402 to Sprunk at 2:26-3:8.

Claim 17 ('661 Patent)	U.S. 5,944,833 to Ugon
The device of claim 15 wherein said source of unpredictable information comprises a hardware random number generator.	8:39-52 – "Thus, a random number generator represented in FIGS. 7A and 7B is constituted, for example, by a set of cells (B0 through B7) each of which is formed by an exclusive OR gate (23) with two inputs connected to a type D switch (24) whose output (Q) is connected to one of the two inputs of the exclusive OR gate of the next cell. The second input of the exclusive OR gate receives the input signal of the data issuing from the bus (3) in order to allow the initial loading or, for the cells (B0) and (B3), for example, a loop-back signal (25) issuing from the last cell (B7). The output (22) of the last cell (B7) also constitutes the output which delivers the pulse signal (I) of randomly variable periodicity. This signal (I) is then used in the calibration circuit (9) represented in FIG. 3A." 10:15-20 – "Another way to produce a generator of this type is to amplify the voltage generated at the terminals of a so-called 'noise' diode and to shape the signals after a low pass filtering for preventing the noise pulses that are too rapid from disturbing the operation." Figure 7A.

Claim 18 ('661 Patent)	U.S. 5,944,833 to Ugon
The device of claim 15 further comprising a monitor for detecting a clock fault in said external clock signal and preventing said processor from processing said quantity if said clock fault is detected.	2:3-7 – "One of the objects of the invention is to equip the circuit with means for preventing the type of investigation described above, and more generally for preventing observations, whether illicit or not, of the internal behavior of the circuit." *See also* U.S. Patent Number 5,249,294 to Griffin et al. at, for example, 2:24-29 and 4:40-5:43.

Claim 19 ('661 Patent)	U.S. 5,944,833 to Ugon
The device of claim 15 wherein said clock decorrelator is selectively operable	2:43-44 – "According to another characteristic, the main program can enable or disable one or more decorrelation means." 5:50-60 – "Thus, the variant of embodiment represented in FIG. 1

under the control of said processor.	allows the main program (5) to change the desired degrees of protection, either by triggering the sequencing of the execution of one or more instructions with the aid of the decorrelated clock CLK2, or by deciding during the execution of an instruction sequence to introduce, or not to introduce, a randomly triggered interrupt handler, or by deciding during the execution of the sequence to introduce, or not to introduce, a jump to the secondary program (6), which also generates a process with a variable time, or even by combining these various possibilities." Claim 12 – "The integrated circuit according to claim 4, characterized in that the main program can enable or disable the decorrelation means."

Claim 20 ('661 Patent)	**U.S. 5,944,833 to Ugon**
The device of claim 15 wherein said clock decorrelator is selectively operable such that said clock decorrelator is disabled when data is being transferred across said input/output interface and enabled during said cryptographic processing operation.	2:43-44 – "According to another characteristic, the main program can enable or disable one or more decorrelation means." 5:50-60 – "Thus, the variant of embodiment represented in FIG. 1 allows the main program (5) to change the desired degrees of protection, either by triggering the sequencing of the execution of one or more instructions with the aid of the decorrelated clock CLK2, or by deciding during the execution of an instruction sequence to introduce, or not to introduce, a randomly triggered interrupt handler, or by deciding during the execution of the sequence to introduce, or not to introduce, a jump to the secondary program (6), which also generates a process with a variable time, or even by combining these various possibilities." 7:66-8:1 – "In another embodiment, the random number generator and the phase shifting circuit can be used continuously during certain particularly sensitive periods . . . ." 9:43-48 – "When the main program executes functions that are not sensitive from the point of view of security, it can also return to the external clock CLKE, for example in order to deliver output data to the external world or to mask the decorrelation interrupt in order to optimize the processing time." Claim 12 – "The integrated circuit according to claim 4, characterized in that the main program can enable or disable the decorrelation means."

Claim 21 ('661 Patent)	U.S. 5,944,833 to Ugon
The device of claim 15 further comprising a noise production system connected to said processor for introducing noise into said measurement of the power consumption by consuming a random amount of power during said cryptographic prosing operation.	5:46-60 – "Lastly, the device of the invention can also comprise a secondary program (6) which, as will be seen below, can generate a variable duration time which varies each time this secondary program (6) is called by the main program (5). Thus, the variant of embodiment represented in FIG. 1 allows the main program (5) to change the desired degrees of protection, either by triggering the sequencing of the execution of one or more instructions with the aid of the decorrelated clock CLK2, or by deciding during the execution of an instruction sequence to introduce, or not to introduce, a randomly triggered interrupt handler, or by deciding during the execution of the sequence to introduce, or not to introduce, a jump to the secondary program (6), which also generates a process with a variable time, or even by combining these various possibilities." 6:66-7:10 – "Another embodiment of a secondary program of variable duration can be comprised of defining an area of the program storage corresponding to the secondary program (6) in which a set of instructions is stored. Preferably, the instructions chosen require different numbers of machine cycles in order to be executed, as is known to be the case, for example, with the instructions J, CALL, RET, RST, PCHL, INX in relation to instructions requiring a number of shorter machine cycles such as ADC, SUB, ANA, MOV, etc. Thus, in this storage area, there are a certain number of available instructions having execution durations that are different from one another in terms of the number of machine cycles." Claim 1 – "A process including a main program having interrupt sequences arranged to execute at least one operation and at least one instruction sequence in a microprocessor in synchronization with internal or external electrical signals of an integrated circuit comprising means for decorrelating an execution of the at least one instruction sequence of the program from the internal or external electrical signals of the integrated circuit so that the execution of the at least one instruction sequence is desynchronized with respect to the internal or external electrical signals, characterized in that the process comprises at least one of the following steps: a) triggering the sequencing of one of at least one instruction or at least one operation with the aid of a random-pulse clock; b) randomly triggering the interrupt sequences; c) triggering the processing of a random sequence of instructions or operations during the execution of a main sequence of instructions or operations; d) combining at least two of steps a, b and c."

Claim 22 ('661 Patent)	U.S. 5,944,833 to Ugon
A device according to claims 1, 4, 7, 9, 11, 14, 15, or 20 wherein said device comprises a smartcard.	3:59-63 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers."

Claim 23 ('661 Patent)	U.S. 5,944,833 to Ugon
A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring, comprising:	*See supra* disclosure regarding preamble of '661 patent claim 1.
(a) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	*See supra* disclosure regarding '661 patent claim 1(a).
(b) generating unpredictable information;	*See supra* disclosure regarding '661 patent claim 1(b).
(c) cryptographically processing said quantity, including using said unpredictable information while processing said quantity to conceal a correlation between externally monitorable signals and said secret by selecting between:	*See supra* disclosure regarding '661 patent claim 1(c)(i).

(c)(1) performing a computation and incorporating the result of said computation in said cryptographic processing, and	2:28-31 – "According to another characteristic, the decorrelation means comprise the execution of secondary sequences in which the instructions and execution times are different and which are selected at random." 8:15-22 – "It is clear that the secondary program can be used to perform functions other than a simple time-out, particularly by executing processes which may be necessary to the main program in order to make use of the time dedicated to the secondary program, which processes can be constituted, for example, by preparations of calculations subsequently used by the main program."
(c)(2) performing a computation whose output is not incorporated in said cryptographic processing; and	2:35-38 – "According to another characteristic, the secondary process does not modify the general operational context of the main program, thus making it possible to return to the latter without having to re-establish this context." 5:46-60 – "Lastly, the device of the invention can also comprise a secondary program (6) which, as will be seen below, can generate a variable duration time which varies each time this secondary program (6) is called by the main program (5). Thus, the variant of embodiment represented in FIG. 1 allows the main program (5) to change the desired degrees of protection, either by triggering the sequencing of the execution of one or more instructions with the aid of the decorrelated clock CLK2, or by deciding during the execution of an instruction sequence to introduce, or not to introduce, a randomly triggered interrupt handler, or by deciding during the execution of the sequence to introduce, or not to introduce, a jump to the secondary program (6), which also generates a process with a variable time, or even by combining these various possibilities."
(d) outputting said cryptographically processed quantity to a recipient thereof.	*See supra* disclosure regarding '661 patent claim 1(d).

Claim 24 ('661 Patent)	**U.S. 5,944,833 to Ugon**
The method of claim 23 where said selecting is performed in software.	5:20-45 – "The device can also comprise a register R2 which is loaded, either by the random number generator (2) with a random number, or by the main program (5) with a value determined by the program. This register R2 is totally or partially used by a logic circuit (4) for triggering an interrupt, which receives at one of its inputs the decorrelated clock signal CLK2 issuing from the output (95) of the

	calibration circuit (9). The output of the circuit (4) is sent through a gate (48) controlled by one or more bits of the register (8) to the interrupt input (12) of the CPU. The bit or bits of this register (8) play the role of an interrupt mask control, which is standard in certain microprocessors. When an interrupt is received at the interrupt input (12) of the processor, the interrupt handling program contained, for example, in the operating system or in the secondary program will introduce a different processing time for the interrupted sequence of the main program. It must be understood that there are two phases in the interrupt mode of operation. A first phase, in which the microprocessor controlled by the so-called main program authorizes the decorrelated operation by unmasking, for example, the interrupts. A second phase, in which the interrupt automatically reroutes the operation to the secondary program. This operation can actually occur without the intervention of the main program." 5:46-60 – "Lastly, the device of the invention can also comprise a secondary program (6) which, as will be seen below, can generate a variable duration time which varies each time this secondary program (6) is called by the main program (5). Thus, the variant of embodiment represented in FIG. 1 allows the main program (5) to change the desired degrees of protection, either by triggering the sequencing of the execution of one or more instructions with the aid of the decorrelated clock CLK2, or by deciding during the execution of an instruction sequence to introduce, or not to introduce, a randomly triggered interrupt handler, or by deciding during the execution of the sequence to introduce, or not to introduce, a jump to the secondary program (6), which also generates a process with a variable time, or even by combining these various possibilities." *See also* 5:49-6:65.

Claim 25 ('661 Patent)	**U.S. 5,944,833 to Ugon**
The method of claim 23 where said selecting is performed in hardware on an integrated circuit including a microprocessor.	5:20-45 – "The device can also comprise a register R2 which is loaded, either by the random number generator (2) with a random number, or by the main program (5) with a value determined by the program. This register R2 is totally or partially used by a logic circuit (4) for triggering an interrupt, which receives at one of its inputs the decorrelated clock signal CLK2 issuing from the output (95) of the calibration circuit (9). The output of the circuit (4) is sent through a gate (48) controlled by one or more bits of the register (8) to the interrupt input (12) of the CPU. The bit or bits of this register (8) play the role of an interrupt mask control, which is standard in certain

	microprocessors. When an interrupt is received at the interrupt input (12) of the processor, the interrupt handling program contained, for example, in the operating system or in the secondary program will introduce a different processing time for the interrupted sequence of the main program. It must be understood that there are two phases in the interrupt mode of operation. A first phase, in which the microprocessor controlled by the so-called main program authorizes the decorrelated operation by unmasking, for example, the interrupts. A second phase, in which the interrupt automatically reroutes the operation to the secondary program. This operation can actually occur without the intervention of the main program." 5:46-60 – "Lastly, the device of the invention can also comprise a secondary program (6) which, as will be seen below, can generate a variable duration time which varies each time this secondary program (6) is called by the main program (5). Thus, the variant of embodiment represented in FIG. 1 allows the main program (5) to change the desired degrees of protection, either by triggering the sequencing of the execution of one or more instructions with the aid of the decorrelated clock CLK2, or by deciding during the execution of an instruction sequence to introduce, or not to introduce, a randomly triggered interrupt handler, or by deciding during the execution of the sequence to introduce, or not to introduce, a jump to the secondary program (6), which also generates a process with a variable time, or even by combining these various possibilities." *See also* 5:49-6:65.

Claim 26 ('661 Patent)	**U.S. 5,944,833 to Ugon**
A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring, comprising:	Abstract – "The present invention relates to an improved integrated circuit for a microprocessor controlled by at least one program and the process for using the circuit which includes means which can decorrelate the running of at least one instruction sequence of a program from internal or external electrical signals of the integrated circuit." 1:44-60 – "This capability of being able to observe the running of a program in a microprocessor or a microcomputer is a major drawback when the microprocessor or microcomputer is used in high-security applications. In effect, an ill-intentioned individual would thus be able to know the successive states of the processor and use this information to gain knowledge of certain internal output data. It is possible to imagine, for example, that a given action on an external

	signal could take place at different instants as a function of the result of a determined security operation, such as the testing of confidential internal information or the decryption of a message, or even the integrity checking of certain information. Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used." 1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 2:2-7 – "One of the objects of the invention is to equip the circuit with means for preventing the type of investigation described above, and more generally for preventing observations, whether illicit or not, of the internal behavior of the circuit." 2:8-11 – "This object is achieved through the fact that the improved integrated circuit has means for decorrelating the running of at least one instruction sequence of a program from the internal or external signals of the circuit." 2:12-13 – "According to another characteristic, the electrical signals of the circuit are timing, synchronization or status signals." 3:59-63 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers." Claim 1 – "A process including a main program having interrupt sequences arranged to execute at least one operation and at least one instruction sequence in a microprocessor in synchronization with internal or external electrical signals of an integrated circuit comprising means for decorrelating an execution of the at least one instruction sequence of the program from the internal or external electrical signals of the integrated circuit so that the execution of the at least one instruction sequence is desynchronized with respect to the internal or external electrical signals . . . ."
(a) receiving a quantity to be cryptographically	1:44-60 – "This capability of being able to observe the running of a program in a microprocessor or a microcomputer is a major drawback when the microprocessor or microcomputer is used in high-security

processed, said quantity being representative of at least a portion of a message;	applications. In effect, an ill-intentioned individual would thus be able to know the successive states of the processor and use this information to gain knowledge of certain internal output data. It is possible to imagine, for example, that a given action on an external signal could take place at different instants as a function of the result of a determined security operation, such as the testing of confidential internal information or the decryption of a message, or even the integrity checking of certain information. Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used." 1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 3:51-58 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories." 3:59-4:3 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers. However, these microcomputers or microprocessors, which use a shift register with parallel input-outputs looped back to at least one of its inputs, wherein the shift is timed by an internal clock, to constitute the random number generator, use the external clock for sequencing the machine cycles of the microprocessor to execute the instruction to read the contents of the register." 4:40-44 – "In the invention, the random number generator (2) is used either to supply a random value to the various devices through the data bus (3) and load it into the various devices which will be described below, or to generate a pulse signal of variable periodicity at its output (22)." *See also* Figures 1, 2 (*e.g.*, element 3).

	Claim 7 – "The integrated circuit according to claim 4, characterized in that said integrated circuit includes logic circuits and connecting busses connected such that sequencing of operations of the microprocessor factors in times required to access logic circuits of the integrated circuit, including signal propagation times in the busses and through the logic circuits." *See also* U.S. Patent No. 5,068,894 (Issued Nov. 26, 1991) at, *e.g.*, 5:4-29.
(b) generating unpredictable information;	2:8-11 – "This object is achieved through the fact that the improved integrated circuit has means for decorrelating the running of at least one instruction sequence of a program from the internal or external signals of the circuit." 2:14-34 – "According to another characteristic, the decorrelation means comprise one or more circuits generating a sequence of clock or timing pulses which are dispatched at random times. According to another characteristic, the decorrelation means comprise a random number generator which makes it possible to de-synchronize the execution of the program sequence in the processor . . . . According to another characteristic, the decorrelation means comprise a random interrupt generating system. According to another characteristic, the decorrelation means comprise the execution of secondary sequences in which the instructions and execution times are different and which are selected at random. According to another characteristic, the variable time of the secondary process depends on a value supplied by a random number generator." 3:59-61 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) . . . ." 4:40-48 – "In the invention, the random number generator (2) is used either to supply a random value to the various devices through the data bus (3) and load it into the various devices which will be described below, or to generate a pulse signal of variable periodicity at its output (22). In a microprocessor or microcomputer of the invention, the signals required for the loading and execution of the instructions can therefore be generated from randomly dispatched clock pulses . . . ." 9:55-10:20 – "For the random number generator (2), it is possible, for example, to use looped counters having different periods, which counters are initialized with a 'seed' (information) stored in a non-volatile memory (7). When the processor starts up, the counters factor in the stored value as the initial value. During the calculation, or at the end of the calculation, the non-volatile memory (7) is updated

	with a new value which will serve as a seed for initializing the counters at the next initialization. The interrupt generating circuit (4) can be designed so that the generation of interrupt pulses seen above can occur, for example, when the number generated has certain characteristics, such as equality with certain data of the program. This circuit (4) can also take on the value of one or more bits of one or more counters. It is also possible to produce a very good random number generator using a cryptographic algorithm (69), as shown in FIG. 5 or a hash function initialized by the 'seeds' (information) seen above. In this case, the generator can be in the form of a program which implements the algorithm executed by the processor (1) and which, for example, implements the cryptographic algorithm by receiving a variable stored in the non-volatile memory (7) and a key for generating an output stored in a buffer register (41). This output stored in the buffer register is then processed by a hardware or software decoding device (42) for generating either the decorrelated clock signal (IT) CLK2 or a signal for interrupting the processor (1). It is easy to see that this random number generator can also be used to generate the various random numbers seen above. Another way to produce a generator of this type is to amplify the voltage generated at the terminals of a so-called 'noise' diode and to shape the signals after a low pass filtering for preventing the noise pulses that are too rapid from disturbing the operation." Figures 1, 2, 4A, 7A, 7B. *See also* 2:48-50, 2:55-57, 2:63-65, 8:39-52.
(c) cryptographically processing said quantity, including using said unpredictable information while processing said quantity to conceal a correlation between externally monitorable signals and said secret	1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 3:51-58 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories." 3:59-63 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family

	of microcomputers."
by selecting a code process from a plurality of code processes, where said selected code process is involved in said cryptographic processing,	2:28-31 – "According to another characteristic, the decorrelation means comprise the execution of secondary sequences in which the instructions and execution times are different and which are selected at random." 5:46-67 –"Lastly, the device of the invention can also comprise a secondary program (6) which, as will be seen below, can generate a variable duration time which varies each time this secondary program (6) is called by the main program (5). Thus, the variant of embodiment represented in FIG. 1 allows the main program (5) to change the desired degrees of protection, either by triggering the sequencing of the execution of one or more instructions with the aid of the decorrelated clock CLK2, or by deciding during the execution of an instruction sequence to introduce, or not to introduce, a randomly triggered interrupt handler, or by deciding during the execution of the sequence to introduce, or not to introduce, a jump to the secondary program (6), which also generates a process with a variable time, or even by combining these various possibilities. Thus, in a variant of the invention, this secondary program (6) can be constituted as represented in FIG. 8 by a plurality of sequences (61, 62, 63 . . . 6n) which are called at random; and each sequence (0, 1, 2 or 2^{n-1}) will implement a different set of instructions which will result in a variable processing time in each branch and different behaviors of the microprocessor." 8:15-22 – "It is clear that the secondary program can be used to perform functions other than a simple time-out, particularly by executing processes which may be necessary to the main program in order to make use of the time dedicated to the secondary program, which processes can be constituted, for example, by preparations of calculations subsequently used by the main program."
but where the value of said outputted quantity is independent of which of said code processes was selected; and	2:35-42 – "According to another characteristic, the secondary process does not modify the general operational context of the main program, thus making it possible to return to the latter without having to re-establish this context. According to another characteristic, the secondary process re-establishes the context of the main program before returning the control of the processor to it." Claim 10 – "The integrated circuit according to claim 8, characterized in that the secondary program sequence does not modify a general operational context of the main program, thus making it possible to return to the main program without having to re-establish the general operational context, wherein the general operational context includes

	at least a next instruction following a last instruction executed."
(d) outputting said cryptographically processed quantity to a recipient thereof.	1:56-60 – "Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used." 1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 3:51-4:3 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories. The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers. However, these microcomputers or microprocessors, which use a shift register with parallel input-outputs looped back to at least one of its inputs, wherein the shift is timed by an internal clock, to constitute the random number generator, use the external clock for sequencing the machine cycles of the microprocessor to execute the instruction to read the contents of the register." *See also* Figures 1, 2 (*e.g.*, element 3). Claim 7 – "The integrated circuit according to claim 4, characterized in that said integrated circuit includes logic circuits and connecting busses connected such that sequencing of operations of the microprocessor factors in times required to access logic circuits of the integrated circuit, including signal propagation times in the busses and through the logic circuits." *See also* U.S. Patent No. 5,068,894 (Issued Nov. 26, 1991) at, *e.g.*, 5:4-29.

Claim 27 ('661 Patent)	U.S. 5,944,833 to Ugon
A method of securely performing a cryptographic processing operation including a sequence of instructions in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring, comprising:	Abstract – "The present invention relates to an improved integrated circuit for a microprocessor controlled by at least one program and the process for using the circuit which includes means which can decorrelate the running of at least one instruction sequence of a program from internal or external electrical signals of the integrated circuit." 1:44-60 – "This capability of being able to observe the running of a program in a microprocessor or a microcomputer is a major drawback when the microprocessor or microcomputer is used in high-security applications. In effect, an ill-intentioned individual would thus be able to know the successive states of the processor and use this information to gain knowledge of certain internal output data. It is possible to imagine, for example, that a given action on an external signal could take place at different instants as a function of the result of a determined security operation, such as the testing of confidential internal information or the decryption of a message, or even the integrity checking of certain information. Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used." 1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 2:2-7 – "One of the objects of the invention is to equip the circuit with means for preventing the type of investigation described above, and more generally for preventing observations, whether illicit or not, of the internal behavior of the circuit." 2:8-11 – "This object is achieved through the fact that the improved integrated circuit has means for decorrelating the running of at least one instruction sequence of a program from the internal or external signals of the circuit." 2:12-13 – "According to another characteristic, the electrical signals of the circuit are timing, synchronization or status signals." 3:59-63 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as

	mentioned above, are particularly known through the ST16XY family of microcomputers." Claim 1 – "A process including a main program having interrupt sequences arranged to execute at least one operation and at least one instruction sequence in a microprocessor in synchronization with internal or external electrical signals of an integrated circuit comprising means for decorrelating an execution of the at least one instruction sequence of the program from the internal or external electrical signals of the integrated circuit so that the execution of the at least one instruction sequence is desynchronized with respect to the internal or external electrical signals . . . ."
(a) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	1:44-60 – "This capability of being able to observe the running of a program in a microprocessor or a microcomputer is a major drawback when the microprocessor or microcomputer is used in high-security applications. In effect, an ill-intentioned individual would thus be able to know the successive states of the processor and use this information to gain knowledge of certain internal output data. It is possible to imagine, for example, that a given action on an external signal could take place at different instants as a function of the result of a determined security operation, such as the testing of confidential internal information or the decryption of a message, or even the integrity checking of certain information. Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used." 1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 3:51-58 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories." 3:59-63 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family

	of microcomputers." 3:59-4:3 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers. However, these microcomputers or microprocessors, which use a shift register with parallel input-outputs looped back to at least one of its inputs, wherein the shift is timed by an internal clock, to constitute the random number generator, use the external clock for sequencing the machine cycles of the microprocessor to execute the instruction to read the contents of the register." 4:40-44 – "In the invention, the random number generator (2) is used either to supply a random value to the various devices through the data bus (3) and load it into the various devices which will be described below, or to generate a pulse signal of variable periodicity at its output (22)." *See also* Figures 1, 2 (*e.g.*, element 3). Claim 7 – "The integrated circuit according to claim 4, characterized in that said integrated circuit includes logic circuits and connecting busses connected such that sequencing of operations of the microprocessor factors in times required to access logic circuits of the integrated circuit, including signal propagation times in the busses and through the logic circuits." *See also* U.S. Patent No. 5,068,894 (Issued Nov. 26, 1991) at, *e.g.*, 5:4-29.
(b) generating unpredictable information;	2:8-11 – "This object is achieved through the fact that the improved integrated circuit has means for decorrelating the running of at least one instruction sequence of a program from the internal or external signals of the circuit." 2:14-34 – "According to another characteristic, the decorrelation means comprise one or more circuits generating a sequence of clock or timing pulses which are dispatched at random times. According to another characteristic, the decorrelation means comprise a random number generator which makes it possible to de-synchronize the execution of the program sequence in the processor . . . . According to another characteristic, the decorrelation means comprise a random interrupt generating system. According to another characteristic, the decorrelation means comprise the execution of secondary sequences in which the instructions and execution times are different and which

	are selected at random. According to another characteristic, the variable time of the secondary process depends on a value supplied by a random number generator." 3:59-61 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) . . . ." 4:40-48 – "In the invention, the random number generator (2) is used either to supply a random value to the various devices through the data bus (3) and load it into the various devices which will be described below, or to generate a pulse signal of variable periodicity at its output (22). In a microprocessor or microcomputer of the invention, the signals required for the loading and execution of the instructions can therefore be generated from randomly dispatched clock pulses . . . ." 9:55-10:20 – "For the random number generator (2), it is possible, for example, to use looped counters having different periods, which counters are initialized with a 'seed' (information) stored in a non-volatile memory (7). When the processor starts up, the counters factor in the stored value as the initial value. During the calculation, or at the end of the calculation, the non-volatile memory (7) is updated with a new value which will serve as a seed for initializing the counters at the next initialization. The interrupt generating circuit (4) can be designed so that the generation of interrupt pulses seen above can occur, for example, when the number generated has certain characteristics, such as equality with certain data of the program. This circuit (4) can also take on the value of one or more bits of one or more counters. It is also possible to produce a very good random number generator using a cryptographic algorithm (69), as shown in FIG. 5 or a hash function initialized by the 'seeds' (information) seen above. In this case, the generator can be in the form of a program which implements the algorithm executed by the processor (1) and which, for example, implements the cryptographic algorithm by receiving a variable stored in the non-volatile memory (7) and a key for generating an output stored in a buffer register (41). This output stored in the buffer register is then processed by a hardware or software decoding device (42) for generating either the decorrelated clock signal (IT) CLK2 or a signal for interrupting the processor (1). It is easy to see that this random number generator can also be used to generate the various random numbers seen above. Another way to produce a generator of this type is to amplify the voltage generated at the terminals of a so-called 'noise' diode and to shape the signals after a low pass filtering for preventing the noise pulses that are too rapid from disturbing the operation."

	Figures 1, 2, 4A, 7A, 7B. *See also* 2:48-50, 2:55-57, 2:63-65, 8:39-52.
(c) using said unpredictable information while processing said quantity to conceal a correlation between externally monitorable signals and said secret by using said unpredictable information to modify said sequence; and	1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 3:51-58 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories." 3:59-63 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers."
(d) outputting said cryptographically processed quantity to a recipient thereof.	1:56-60 – "Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used." 1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." *See also* U.S. Patent No. 5,068,894 (Issued Nov. 26, 1991) at, *e.g.*, 5:4-29.

Claim 28 ('661 Patent)	**U.S. 5,944,833 to Ugon**
A method of securely performing a cryptographic	*See supra* disclosure regarding preamble of '661 patent claim 5.

processing operation implementing a permutation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring, comprising:	
(a) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	*See supra* disclosure regarding '661 patent claim 5(a).
(b) generating unpredictable information;	*See supra* disclosure regarding '661 patent claim 5(b).
(c) using said unpredictable information while processing said quantity to conceal a correlation between externally monitorable signals and said secret by randomizing the order of said permutation; and	*See supra* disclosure regarding '661 patent claim 5(c)(ii).
(d) outputting said cryptographically processed quantity to a recipient thereof.	*See supra* disclosure regarding '661 patent claim 5(d).

Claim 29 ('661 Patent)	**U.S. 5,944,833 to Ugon**
A method of securely performing a cryptographic processing operation in	Abstract – "The present invention relates to an improved integrated circuit for a microprocessor controlled by at least one program and the process for using the circuit which includes means which can decorrelate the running of at least one instruction sequence of a

a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring of said device's power consumption, comprising:	program from internal or external electrical signals of the integrated circuit." 1:44-60 – "This capability of being able to observe the running of a program in a microprocessor or a microcomputer is a major drawback when the microprocessor or microcomputer is used in high-security applications. In effect, an ill-intentioned individual would thus be able to know the successive states of the processor and use this information to gain knowledge of certain internal output data. It is possible to imagine, for example, that a given action on an external signal could take place at different instants as a function of the result of a determined security operation, such as the testing of confidential internal information or the decryption of a message, or even the integrity checking of certain information. Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used." 1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 2:2-7 – "One of the objects of the invention is to equip the circuit with means for preventing the type of investigation described above, and more generally for preventing observations, whether illicit or not, of the internal behavior of the circuit." 2:8-11 – "This object is achieved through the fact that the improved integrated circuit has means for decorrelating the running of at least one instruction sequence of a program from the internal or external signals of the circuit." 2:12-13 – "According to another characteristic, the electrical signals of the circuit are timing, synchronization or status signals." 3:59-63 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers." Claim 1 – "A process including a main program having interrupt sequences arranged to execute at least one operation and at least one instruction sequence in a microprocessor in synchronization with

	internal or external electrical signals of an integrated circuit comprising means for decorrelating an execution of the at least one instruction sequence of the program from the internal or external electrical signals of the integrated circuit so that the execution of the at least one instruction sequence is desynchronized with respect to the internal or external electrical signals . . . ."
(a) receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	1:44-60 – "This capability of being able to observe the running of a program in a microprocessor or a microcomputer is a major drawback when the microprocessor or microcomputer is used in high-security applications. In effect, an ill-intentioned individual would thus be able to know the successive states of the processor and use this information to gain knowledge of certain internal output data. It is possible to imagine, for example, that a given action on an external signal could take place at different instants as a function of the result of a determined security operation, such as the testing of confidential internal information or the decryption of a message, or even the integrity checking of certain information. Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used." 2:8-13 – "This object is achieved through the fact that the improved integrated circuit has means for decorrelating the running of at least one instruction sequence of a program from the internal or external signals of the circuit. According to another characteristic, the electrical signals of the circuit are timing, synchronization or status signals." 1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 3:51-58 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories." 3:59-63 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned

	above, are particularly known through the ST16XY family of microcomputers." Claim 2 – "An integrated circuit comprising a microprocessor controlled by at least one program including at least one program interrupt, the at least one program being arranged to execute at least one instruction sequence in the microprocessor in synchronization with internal or external electrical signals of the integrated circuit and means for decorrelating execution of the at least one instruction sequence of the program from the internal or external electrical signals of the integrated circuit so that the execution of the at least one instruction sequence is desynchronized with respect to the internal or external electrical signals and the program having an instruction sequence for authorization, modification, or disablement of the decorrelation means, wherein authorization includes unmasking the program interrupts." *See also* U.S. Patent No. 5,068,894 (Issued Nov. 26, 1991) at, *e.g.*, 5:4-29.
(b) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;	1:44-60 – "This capability of being able to observe the running of a program in a microprocessor or a microcomputer is a major drawback when the microprocessor or microcomputer is used in high-security applications. In effect, an ill-intentioned individual would thus be able to know the successive states of the processor and use this information to gain knowledge of certain internal output data. It is possible to imagine, for example, that a given action on an external signal could take place at different instants as a function of the result of a determined security operation, such as the testing of confidential internal information or the decryption of a message, or even the integrity checking of certain information. Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used." 1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 3:51-58 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a

	ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories." 3:59-63 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers." *See also* U.S. Patent No. 5,068,894 (Issued Nov. 26, 1991) at, *e.g.*, 5:4-29.
(c) introducing noise into said measurement of said power consumption while processing said quantity; and	Abstract – "The present invention relates to an improved integrated circuit for a microprocessor controlled by at least one program and the process for using the circuit which includes means which can decorrelate the running of at least one instruction sequence of a program from internal or external electrical signals of the integrated circuit." 3:59-61 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) . . . ." 2:14-34 – "According to another characteristic, the decorrelation means comprise one or more circuits generating a sequence of clock or timing pulses which are dispatched at random times. According to another characteristic, the decorrelation means comprise a random number generator which makes it possible to de-synchronize the execution of the program sequence in the processor . . . . According to another characteristic, the decorrelation means comprise a random interrupt generating system. According to another characteristic, the decorrelation means comprise the execution of secondary sequences in which the instructions and execution times are different and which are selected at random. According to another characteristic, the variable time of the secondary process depends on a value supplied by a random number generator." 4:40-48 – "In the invention, the random number generator (2) is used either to supply a random value to the various devices through the data bus (3) and load it into the various devices which will be described below, or to generate a pulse signal of variable periodicity at its output (22). In a microprocessor or microcomputer of the invention, the signals required for the loading and execution of the instructions can therefore be generated from randomly dispatched clock pulses . . . ." Claim 1 – "A process including a main program having interrupt sequences arranged to execute at least one operation and at least one instruction sequence in a microprocessor in synchronization with

	internal or external electrical signals of an integrated circuit comprising means for decorrelating an execution of the at least one instruction sequence of the program from the internal or external electrical signals of the integrated circuit so that the execution of the at least one instruction sequence is desynchronized with respect to the internal or external electrical signals, characterized in that the process comprises at least one of the following steps: a) triggering the sequencing of one of at least one instruction or at least one operation with the aid of a random-pulse clock; b) randomly triggering the interrupt sequences; c) triggering the processing of a random sequence of instructions or operations during the execution of a main sequence of instructions or operations; d) combining at least two of steps a, b and c." Claim 2 – "An integrated circuit comprising a microprocessor controlled by at least one program including at least one program interrupt, the at least one program being arranged to execute at least one instruction sequence in the microprocessor in synchronization with internal or external electrical signals of the integrated circuit and means for decorrelating execution of the at least one instruction sequence of the program from the internal or external electrical signals of the integrated circuit so that the execution of the at least one instruction sequence is desynchronized with respect to the internal or external electrical signals and the program having an instruction sequence for authorization, modification, or disablement of the decorrelation means, wherein authorization includes unmasking the program interrupts."
(d) outputting said cryptographically processed quantity to a recipient thereof.	1:56-60 – "Depending on the instant in question, this external signal could supply information on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used." 1:61-67 – "Moreover, there are known microprocessors or microcomputers, such as those marketed by the company SGS Thomson under the reference number ST16XY, which comprise a microprocessor incorporating a random number generator, the reading of which makes it possible to obtain a random number used, for example, for the calculation of encryptions and decryptions." 3:51-4:3 – "In the following description, the term microcomputer is intended to mean a monolithic integrated circuit incorporating a microprocessor with a read-write memory of the RAM type associated with at least one non-volatile memory which may or may not be programmable such as, for example, a RAM with battery backup, or a ROM, or PROM, or EPROM, or EEPROM, or RAM of the Flash type, etc . . . or a combination of these memories. The invention will

	now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) which can run on an internal clock (11). Processors of this type, as mentioned above, are particularly known through the ST16XY family of microcomputers. However, these microcomputers or microprocessors, which use a shift register with parallel input-outputs looped back to at least one of its inputs, wherein the shift is timed by an internal clock, to constitute the random number generator, use the external clock for sequencing the machine cycles of the microprocessor to execute the instruction to read the contents of the register." *See also* Figures 1, 2 (*e.g.*, element 3). Claim 7 – "The integrated circuit according to claim 4, characterized in that said integrated circuit includes logic circuits and connecting busses connected such that sequencing of operations of the microprocessor factors in times required to access logic circuits of the integrated circuit, including signal propagation times in the busses and through the logic circuits." *See also* U.S. Patent No. 5,068,894 (Issued Nov. 26, 1991) at, *e.g.*, 5:4-29.

Claim 30 ('661 Patent)	**U.S. 5,944,833 to Ugon**
The method of claim 29 wherein said step of introducing noise comprises: (a) generating initial noise having a random characteristic;	*See supra* disclosure regarding '661 patent claim 12(a).
(b) improving the random characteristic of said initial noise; and	*See supra* disclosure regarding '661 patent claim 12(b).
(c) varying said power consumption based on said improved initial noise.	*See supra* disclosure regarding '661 patent claim 12(c).

Claim 31 ('661 Patent)	U.S. 5,944,833 to Ugon
A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring of said device's power consumption, comprising:	*See supra* disclosure regarding preamble of '661 patent claim 14.
(a) receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	*See supra* disclosure regarding '661 patent claim 14(c).
(b) generating a first clock signal;	*See supra* disclosure regarding '661 patent claim 14(d).
(c) receiving data to be cryptographically processed, said data being representative of at least a portion of a message;	*See supra* disclosure regarding '661 patent claim 14(a).
(d) generating unpredictable information;	*See supra* disclosure regarding '661 patent claim 14(d).
(e) generating a second clock signal from said first clock signal using said unpredictable information, such that said second clock signal cannot be reliably predicted from said first clock signal;	*See supra* disclosure regarding '661 patent claim 14(e).

(f) processing said data using said second clock signal; and	*See supra* disclosure regarding '661 patent claim 14(f)(i) and (ii).
(g) outputting said cryptographically processed quantity to a recipient thereof.	*See supra* disclosure regarding '661 patent claim 14(f)(iii).

Claim 32 ('661 Patent)	**U.S. 5,944,833 to Ugon**
A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring of said device's power consumption, comprising:	*See supra* disclosure regarding preamble of '661 patent claim 15.
(a) receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;	*See supra* disclosure regarding '661 patent claim 15(c).
(b) receiving an external clock signal;	*See supra* disclosure regarding '661 patent claim 15(b)
(c) receiving data to be cryptographically processed, said data being representative of at least a portion of a message;	*See supra* disclosure regarding '661 patent claim 15(a).
(d) generating unpredictable	*See supra* disclosure regarding '661 patent claim 15(d).

information;	
(e) generating an internal clock signal from said external clock signal using said unpredictable information, such that said external clock signal cannot be reliably predicted from said internal clock signal;	*See supra* disclosure regarding '661 patent claim 15(e).
(f) processing said data using said internal clock signal; and	*See supra* disclosure regarding '661 patent claim 15(f)(i) and (ii).
(g) outputting said cryptographically processed quantity to a recipient thereof.	*See supra* disclosure regarding '661 patent claim 15(f)(iii).

Claim 33 ('661 Patent)	**U.S. 5,944,833 to Ugon**
The method of claim 32 wherein said step of generating said internal clock signal comprises a step of selecting a subset of the cycles of said external clock signal to use as said internal clock signal based on said unpredictable information.	4:50-63 – "This signal, in order to serve as a clock for the microprocessor (1), must be sent to a calibration circuit (9). The output (95) of this calibration circuit is sent to a multiplexing circuit (18) whose input (19) for controlling the multiplexing receives the signal of one or more bits of a register (8) which can be loaded either by the random number generator (2) or with a value determined by the main program (5). When this register (8) is loaded with a random value, the decision which selects the clock signal sent to the processor is made randomly, whereas when this register (8) is loaded with a value determined by the main program, it is the main program which will choose whether the clock for sequencing the microprocessor will be the external clock CLKE or a decorrelation clock CLK2." *See also* U.S. Patent Number 5,404,402 to Sprunk at 2:26-3:8; Posting of Jim Bell to sci.crypt newsgroup, http://groups.google.com/group/sci.crypt/msg/485abca33cc29703?dmode=source&hl=en (December 24, 1995), last visited November 17, 2006.

Claim 34 ('661 Patent)	U.S. 5,944,833
The method of claim 32 wherein said step of generating unpredictable information comprises a step of generating a random number.	2:8-11 – "This object is achieved through the fact that the improved integrated circuit has means for decorrelating the running of at least one instruction sequence of a program from the internal or external signals of the circuit." 2:14-34 – "According to another characteristic, the decorrelation means comprise one or more circuits generating a sequence of clock or timing pulses which are dispatched at random times. According to another characteristic, the decorrelation means comprise a random number generator which makes it possible to de-synchronize the execution of the program sequence in the processor . . . . According to another characteristic, the decorrelation means comprise a random interrupt generating system. According to another characteristic, the decorrelation means comprise the execution of secondary sequences in which the instructions and execution times are different and which are selected at random. According to another characteristic, the variable time of the secondary process depends on a value supplied by a random number generator." 3:59-61 – "The invention will now be explained with the aid of FIG. 1 in which a CPU (1) comprises a random number generator (2) . . . ." 4:40-48 – "In the invention, the random number generator (2) is used either to supply a random value to the various devices through the data bus (3) and load it into the various devices which will be described below, or to generate a pulse signal of variable periodicity at its output (22). In a microprocessor or microcomputer of the invention, the signals required for the loading and execution of the instructions can therefore be generated from randomly dispatched clock pulses . . . ." 9:55-10:20 – "For the random number generator (2), it is possible, for example, to use looped counters having different periods, which counters are initialized with a 'seed' (information) stored in a non-volatile memory (7). When the processor starts up, the counters factor in the stored value as the initial value. During the calculation, or at the end of the calculation, the non-volatile memory (7) is updated with a new value which will serve as a seed for initializing the counters at the next initialization. The interrupt generating circuit (4) can be designed so that the generation of interrupt pulses seen above can occur, for example, when the number generated has certain characteristics, such as equality with certain data of the program. This circuit (4) can also take on the value of one or more bits of one or more counters. It is also possible to produce a very good random number generator using a cryptographic algorithm (69), as shown in FIG. 5 or a hash function initialized by the 'seeds' (information) seen above. In this case, the

	generator can be in the form of a program which implements the algorithm executed by the processor (1) and which, for example, implements the cryptographic algorithm by receiving a variable stored in the non-volatile memory (7) and a key for generating an output stored in a buffer register (41). This output stored in the buffer register is then processed by a hardware or software decoding device (42) for generating either the decorrelated clock signal (IT) CLK2 or a signal for interrupting the processor (1). It is easy to see that this random number generator can also be used to generate the various random numbers seen above. Another way to produce a generator of this type is to amplify the voltage generated at the terminals of a so-called 'noise' diode and to shape the signals after a low pass filtering for preventing the noise pulses that are too rapid from disturbing the operation." Figures 1, 2, 4A, 7A, 7B. *See also* 2:48-50, 2:55-57, 2:63-65, 8:39-52.

Claim 35 ('661 Patent)	**U.S. 5,944,833 to Ugon**
The method of claim 32 further comprising a step of monitoring for a clock fault in said external clock signal and a step of preventing said processor from outputting said cryptographically processed quantity if said clock fault is detected.	2:3-7 – "One of the objects of the invention is to equip the circuit with means for preventing the type of investigation described above, and more generally for preventing observations, whether illicit or not, of the internal behavior of the circuit." *See also* U.S. Patent Number 5,249,294 to Griffin et al. at, for example, 2:24-29 and 4:40-5:43.

Claim 36 ('661 Patent)	**U.S. 5,944,833 to Ugon**
The method of claim 32 further comprising a step of introducing noise into said measurement of the power consumption.	*See supra* disclosure regarding '661 patent claim 21.